

MP-2131

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICANT(S): Shinako Matsuyama, et al. ATTY. DOCKET NO. 09792909-5002

SERIAL NO. 09/843,403 GROUP ART UNIT: 2131

DATE FILED: April 26, 2001 EXAMINER:

INVENTION: "ACCESS CONTROL SYSTEM, ACCESS CONTROL METHOD, DEVICE, ACCESS CONTROL SERVER, ACCESS-CONTROL-SERVER, REGISTRATION SERVER, DATA PROCESSING APPARATUS, AND PROGRAM STORAGE MEDIUM"



SUBMISSION OF CERTIFIED COPY OF PRIORITY DOCUMENT

Assistant Commissioner of Patents
Washington, D.C. 20231

RECEIVED

AUG 28 2001

S I R:

Technology Center 2100

Applicants herewith submit the certified copies of Japanese Applications Nos. P2000-125787 filed April 26, 2000, and P2001-089672 filed March 27, 2001, and claims priority to the April 26, 2000, date.

The Commissioner is authorized to charge any fees which may be due or credit any overpayments to Deposit Account No. 19-3140. A duplicate copy of this sheet is enclosed for that purpose.

Respectfully submitted,

A handwritten signature of David R. Metzger in cursive script.

(Reg. No. 32,919)

David R. Metzger
SONNENSCHN NATH & ROSENTHAL
P.O. Box #061080
Wacker Drive Station - Sears Tower
Chicago, Illinois 60606-1080
Telephone 312/876-8000
Customer #26263
Attorneys for Applicants

CERTIFICATE OF MAILING

I hereby certify that a true copy of the foregoing Submission of Certified Copies of Priority Documents was forwarded to the United States Patent Office via U.S. First Class mail on August 21, 2001.

A handwritten signature of David R. Metzger in cursive script, followed by a horizontal line.

501P0625US00

RECEIVED

AUG 28 2001

Technology Center 2100



日本国特許庁

PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日

Date of Application:

2000年 4月26日

出願番号

Application Number:

特願2000-125787

出願人

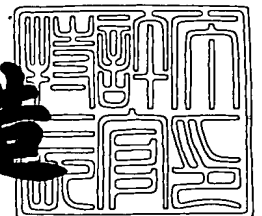
Applicant (s):

ソニー株式会社

2001年 3月 9日

特許庁長官
Commissioner,
Patent Office

及川耕造



出証番号 出証特2001-3016439

【書類名】 特許願

【整理番号】 00001536

【提出日】 平成12年 4月26日

【あて先】 特許庁長官殿

【国際特許分類】 H04L 9/32

【発明の名称】 アクセス制御システムおよびアクセス制御方法、並びに
プログラム提供媒体

【請求項の数】 26

【発明者】

【住所又は居所】 東京都品川区北品川6丁目7番35号 ソニー株式会社
内

【氏名】 松山 科子

【発明者】

【住所又は居所】 東京都品川区北品川6丁目7番35号 ソニー株式会社
内

【氏名】 石橋 義人

【発明者】

【住所又は居所】 東京都品川区北品川6丁目7番35号 ソニー株式会社
内

【氏名】 二村 一郎

【発明者】

【住所又は居所】 東京都品川区北品川6丁目7番35号 ソニー株式会社
内

【氏名】 昆 雅士

【発明者】

【住所又は居所】 東京都品川区北品川6丁目7番35号 ソニー株式会社
内

【氏名】 渡辺 秀明

【特許出願人】

【識別番号】 000002185
【氏名又は名称】 ソニー株式会社
【代表者】 出井 伸之

【代理人】

【識別番号】 100101801
【弁理士】
【氏名又は名称】 山田 英治
【電話番号】 03-5541-7577

【選任した代理人】

【識別番号】 100093241
【弁理士】
【氏名又は名称】 宮田 正昭
【電話番号】 03-5541-7577

【選任した代理人】

【識別番号】 100086531
【弁理士】
【氏名又は名称】 澤田 俊夫
【電話番号】 03-5541-7577

【手数料の表示】

【予納台帳番号】 062721
【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1
【物件名】 図面 1
【物件名】 要約書 1
【包括委任状番号】 9904833

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 アクセス制御システムおよびアクセス制御方法、並びにプログラム提供媒体

【特許請求の範囲】

【請求項 1】

公開鍵証明書発行局が認証対象に発行する公開鍵証明書を利用して公開鍵系暗号方式を使用したデータ転送を行なうデータ転送システムにおけるアクセス制御システムにおいて、

前記認証対象であり、サービスを提供するサービスプロバイダと、

前記認証対象であり、前記サービスプロバイダの提供するサービスを受領するサービス受領デバイスと、

前記サービス受領デバイスのアクセスが許可されたサービスプロバイダを識別可能なアクセス許可書を前記サービス受領デバイスに対して発行するアクセス制御サーバと、を有し、

前記サービス提供プロバイダは、前記サービス受領デバイスからのアクセス要求に対するアクセス許可判定を、前記アクセス許可書に基づいて実行する構成であることを特徴とするアクセス制御システム。

【請求項 2】

前記アクセス制御システムは、さらに、

アクセス制御サーバ登録サーバを有し、

前記アクセス制御サーバ登録サーバは、前記サービス受領デバイスからのアクセス許可書発行要求を受領して、前記アクセス制御サーバに対するアクセス許可書発行処理の実行要求を行なう構成であることを特徴とする請求項 1 に記載のアクセス制御システム。

【請求項 3】

前記アクセス制御システムは、さらに、

ユーザ端末によって利用可能なコンテンツまたはサービスの提供を可能とするコンテンツまたはサービスの流通インフラを提供または管理する機関であるシステムホルダを有し、

前記システムホルダは、前記サービスプロバイダおよびサービス受領デバイスを管轄し、認証対象とした構成であることを特徴とする請求項1に記載のアクセス制御システム。

【請求項4】

前記アクセス制御サーバは、前記システムホルダ各々に対応して設けられ、
前記システムホルダの管轄するサービスプロバイダの提供するサービスに関するアクセス許可書を発行する構成であることを特徴とする請求項3に記載のアクセス制御システム。

【請求項5】

前記アクセス制御サーバは、前記システムホルダの複数に対して共通に設けられ、

該複数のシステムホルダの管轄するサービスプロバイダの提供するサービスに関するアクセス許可書を発行する構成であることを特徴とする請求項3に記載のアクセス制御システム。

【請求項6】

前記アクセス制御システムは、さらに、

前記システムホルダを管轄するルート登録局を有し、

前記ルート登録局は、前記システムホルダからの要求に基づいて該ルート登録局の管轄する認証対象の公開鍵証明書の発行要求を前記公開鍵証明書発行局に対して実行する構成であることを特徴とする請求項3に記載のアクセス制御システム。

【請求項7】

前記アクセス制御サーバは、

前記アクセス許可書を、サービスプロバイダ毎に独立に使用可能な態様で生成することを特徴とする請求項1に記載のアクセス制御システム。

【請求項8】

前記アクセス制御サーバは、

前記アクセス許可書を、複数のサービスプロバイダに共通に使用可能な態様で生成することを特徴とする請求項1に記載のアクセス制御システム。

【請求項9】

前記アクセス制御サーバは、

前記アクセス制御サーバの設定するアクセス制御サーバ設定固定フィールドと

前記サービスプロバイダの各々が設定するサービスプロバイダ設定オプションフィールドと、

前記アクセス制御サーバによる電子署名フィールドと、

から成るフォーマットで、前記アクセス許可書を生成する構成であることを特徴とする請求項1に記載のアクセス制御システム。

【請求項10】

前記サービスプロバイダ設定オプションフィールドには、サービス受領デバイス毎のアクセス可否を決定する識別データを含み、該識別データは、前記サービス受領デバイスのユーザに関する個人情報、ユーザID、ユーザデバイスID、またはアクセス許可識別フラグの少なくともいずれかを含む構成であることを特徴とする請求項9に記載のアクセス制御システム。

【請求項11】

前記サービスプロバイダ、前記サービス受領デバイス、前記アクセス制御サーバ間において、直接あるいは仲介手段を介して実行されるデータ転送は、データ転送相互間における相互認証処理が実行され、相互認証が成立したことを条件としたデータ転送として実行する構成であることを特徴とする請求項1に記載のアクセス制御システム。

【請求項12】

前記サービスプロバイダ、前記サービス受領デバイス、前記アクセス制御サーバ間において、直接あるいは仲介手段を介して実行される転送データはデータ送信側の電子署名が付加されたデータとして転送する構成であることを特徴とする請求項1に記載のアクセス制御システム。

【請求項13】

前記サービスプロバイダは、

サービスを提供するデバイスであることを特徴とする請求項1に記載のアクセ

ス制御システム。

【請求項 14】

前記アクセス制御サーバは、

前記アクセス許可書に設定されたアクセス許可を取り消すアクセス許可書の変更処理を実行する構成であることを特徴とする請求項 1 に記載のアクセス制御システム。

【請求項 15】

公開鍵証明書発行局が認証対象に発行する公開鍵証明書を利用して公開鍵系暗号方式を使用したデータ転送を行なうデータ転送システムにおけるアクセス制御方法であり、

サービス提供プロバイダにおいて、サービス受領デバイスから、サービス制御サーバの発行したアクセス許可書を受領するステップと、

前記アクセス許可書に基づいて、前記サービス受領デバイスのアクセス要求に対するアクセス許可判定を実行するステップと、

を有することを特徴とするアクセス制御方法。

【請求項 16】

前記アクセス制御方法は、さらに、

アクセス制御サーバにおいて、サービス受領デバイスのアクセスが許可されたサービスプロバイダを識別可能なアクセス許可書をサービス受領デバイスに対して発行するアクセス許可書発行ステップと、

を含むことを特徴とする請求項 15 に記載のアクセス制御方法。

【請求項 17】

前記アクセス制御方法は、さらに、

前記アクセス制御サーバ登録サーバにおいて、前記サービス受領デバイスからのアクセス許可書発行要求を受領して、前記アクセス制御サーバに対するアクセス許可書発行処理の実行要求を行なうステップを有することを特徴とする請求項 15 に記載のアクセス制御方法。

【請求項 18】

前記アクセス許可書発行ステップは、

ユーザ端末によって利用可能なコンテンツまたはサービスの提供を可能とするコンテンツまたはサービスの流通インフラを提供または管理する機関であるシステムホルダの管轄するサービスプロバイダからの発行要求に基づいて実行されることを特徴とする請求項 1 5 に記載のアクセス制御方法。

【請求項 1 9】

前記アクセス許可書発行ステップは、

サービスプロバイダ毎に独立に使用可能な態様で前記アクセス許可書を生成することを特徴とする請求項 1 5 に記載のアクセス制御方法。

【請求項 2 0】

前記アクセス許可書発行ステップは、

複数のサービスプロバイダに共通に使用可能な態様で前記アクセス許可書を生成することを特徴とする請求項 1 5 に記載のアクセス制御方法。

【請求項 2 1】

前記アクセス許可書発行ステップは、

前記アクセス制御サーバの設定するアクセス制御サーバ設定固定フィールドと

前記サービスプロバイダの各々が設定するサービスプロバイダ設定オプションフィールドと、

前記アクセス制御サーバによる電子署名フィールドと、

から成るフォーマットで生成することを特徴とする請求項 1 5 に記載のアクセス制御方法。

【請求項 2 2】

前記サービスプロバイダにおいて実行されるアクセス許可判定実行ステップは

前記アクセス許可書に含まれるサービス受領デバイス毎のアクセス可否を決定する識別データとしての前記サービス受領デバイスのユーザに関する個人情報、ユーザ ID, ユーザデバイス ID, またはアクセス許可識別フラグの少なくともいずれかに基づいてアクセス許可の判定を実行することを特徴とする請求項 1 5 に記載のアクセス制御方法。

【請求項 2 3】

前記サービスプロバイダ、前記サービス受領デバイス、前記アクセス制御サーバ間において、直接あるいは仲介手段を介して実行されるデータ転送は、データ転送相互間における相互認証処理を実行し、相互認証が成立したことを条件としたデータ転送として実行することを特徴とする請求項 1 5 に記載のアクセス制御方法。

【請求項 2 4】

前記サービスプロバイダ、前記サービス受領デバイス、前記アクセス制御サーバ間において、直接あるいは仲介手段を介して実行される転送データにはデータ送信側の電子署名を付加することを特徴とする請求項 1 5 に記載のアクセス制御方法。

【請求項 2 5】

前記アクセス制御方法は、さらに、

前記アクセス制御サーバにおいて、

前記アクセス許可書に設定されたアクセス許可を取り消すアクセス許可書の変更処理を実行するアクセス許可書変更処理ステップを含むことを特徴とする請求項 1 5 に記載のアクセス制御方法。

【請求項 2 6】

公開鍵証明書発行局が認証対象に発行する公開鍵証明書を利用して公開鍵系暗号方式を使用したデータ転送を行なうデータ転送システムにおけるアクセス制御処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、

サービス提供プロバイダにおいて、サービス受領デバイスから、サービス制御サーバの発行したアクセス許可書を受領するステップと、

前記アクセス許可書に基づいて、前記サービス受領デバイスのアクセス要求に対するアクセス許可判定を実行するステップと、

を有することを特徴とするプログラム提供媒体。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明はアクセス制御システムおよびアクセス制御方法に関する。特に、様々なサービスプロバイダが提供するサービスへのユーザデバイスからのアクセスに対する制御を行なうアクセス制御システムおよびアクセス制御方法に関する。さらに、詳細には、各エンティティが公開鍵証明書を保有し、公開鍵ベースの相互認証を実行して、データ通信を実行するシステムにおいて有用な、アクセス制御システムおよびアクセス制御方法に関するものである。

【0002】

【従来の技術】

昨今、ゲームプログラム、音声データ、画像データ、文書作成プログラム等、様々なソフトウェアデータ（以下、これらをコンテンツ（Content）と呼ぶ）が、インターネット等のネットワークを介して流通している。また、オンラインショッピング等、ネットワークを介した商品売買も次第に盛んになってきている。

【0003】

このようなネットワークを介したデータ通信においては、データ送信側とデータ受信側とが互いに正規なデータ送受信対象であることを確認した上で、必要な情報を転送する、すなわちセキュリティを考慮したデータ転送構成をとるのが一般的となっている。データ転送の際のセキュリティ構成を実現する1つの手法が、転送データの暗号化処理、データに対する署名処理である。

【0004】

暗号化データは、所定の手続きによる復号化処理によって利用可能な復号データ（平文）に戻すことができる。このような情報の暗号化処理に暗号化鍵を用い、復号化処理に復号化鍵を用いるデータ暗号化、復号化方法は従来からよく知られている。

【0005】

暗号化鍵と復号化鍵を用いるデータ暗号化・復号化方法の態様には様々な種類があるが、その1つの例としていわゆる公開鍵暗号方式と呼ばれる方式がある。公開鍵暗号方式は、発信者と受信者の鍵を異なるものとして、一方の鍵を不特定のユーザが使用可能な公開鍵として、他方を秘密に保つ秘密鍵とするものである。

例えば、データ暗号化鍵を公開鍵とし、復号鍵を秘密鍵とする。あるいは、認証子生成鍵を秘密鍵とし、認証子復号鍵を公開鍵とする等の態様において使用される。

【0006】

暗号化、復号化に共通の鍵を用いるいわゆる共通鍵暗号化方式と異なり、公開鍵暗号方式では秘密に保つ必要のある秘密鍵は、特定の1人が持てばよい。鍵の管理において有利である。ただし、公開鍵暗号方式は共通鍵暗号化方式に比較してデータ処理速度が遅く、秘密鍵の配送、デジタル署名等のデータ量の少ない対象に多く用いられている。公開鍵暗号方式の代表的なものにはRSA (Rivest-Shamir-Adleman) 暗号がある。これは非常に大きな2つの素数（例えば150桁）の積を用いるものであり、大きな2つの素数（例えば150桁）の積の素因数分解する処理の困難さを利用している。

【0007】

公開鍵暗号方式では、不特定多数に公開鍵を使用可能とする構成であり、配布する公開鍵が正当なものであるか否かを証明する証明書、いわゆる公開鍵証明書を使用する方法が多く用いられている。例えば、利用者Aが公開鍵、秘密鍵のペアを生成して、生成した公開鍵を認証局に対して送付して公開鍵証明書を認証局から入手する。利用者Aは公開鍵証明書を一般に公開する。不特定のユーザは公開鍵証明書から所定の手続きを経て公開鍵を入手して文書等を暗号化して利用者Aに送付する。利用者Aは秘密鍵を用いて暗号化文書等を復号する等のシステムである。また、利用者Aは、秘密鍵を用いて文書等に署名を付け、不特定のユーザが公開鍵証明書から所定の手続きを経て公開鍵を入手して、その署名の検証を行なうシステムである。

【0008】

公開鍵証明書について図1を用いて説明する。公開鍵証明書は、公開鍵暗号方式における認証局（CA: Certificate AuthorityまたはIA: Issuer Authority）が発行する証明書であり、ユーザが自己のID、公開鍵等を認証局に提出することにより、認証局側が認証局のIDや有効期限等の情報を付加し、さらに認証局による署名を付加して作成される証明書である。

【0009】

図1に示す公開鍵証明書は、証明書のバージョン番号、認証局（IA）が証明書利用者に対し割り付ける証明書の通し番号、電子署名に用いたアルゴリズムおよびパラメータ、認証局の名前、証明書の有効期限、証明書利用者の名前（ユーザID）、証明書利用者の公開鍵並びに電子署名を含む。

【0010】

電子署名は、証明書のバージョン番号、認証局が証明書利用者に対し割り付ける証明書の通し番号、電子署名に用いたアルゴリズムおよびパラメータ、認証局の名前、証明書の有効期限、証明書利用者の名前並びに証明書利用者の公開鍵全体に対しハッシュ関数を適用してハッシュ値を生成し、そのハッシュ値に対して認証局の秘密鍵を用いて生成したデータである。

【0011】

認証局は、図1に示す公開鍵証明書を発行するとともに、有効期限が切れた公開鍵証明書を更新し、不正を行った利用者の排斥を行うための不正者リストの作成、管理、配布（これをリボケーション：Revocationと呼ぶ）を行う。また、必要に応じて公開鍵・秘密鍵の生成も行う。

【0012】

一方、この公開鍵証明書を利用する際には、利用者は自己が保持する認証局の公開鍵を用い、当該公開鍵証明書の電子署名を検証し、電子署名の検証に成功した後に公開鍵証明書から公開鍵を取り出し、当該公開鍵を利用する。従って、公開鍵証明書を利用する全ての利用者は、共通の認証局の公開鍵を保持している必要がある。

【0013】

【発明が解決しようとする課題】

上述のような認証局発行の公開鍵証明書を用いた公開鍵暗号方式によるデータ送信システムにおいては、使用する公開鍵が異なれば、その公開鍵に対して新たに認証局に対して公開鍵証明書の発行を依頼、あるいは認証局構成を持つ認証システムを構築することが必要となる。すなわち、例えばコンテンツの配信、商品提供サービスを行なうサービスプロバイダは、新たなサービス（新たな電子配信

システム)を開始し、新たな公開鍵の使用を開始する際に、逐一、新たな公開鍵に対応する公開鍵証明書の発行、管理を認証局に依頼、あるいは、新たに認証局構成を持つ認証システムを構築しなければならない、多大なコスト、時間を要するという問題があった。

【 0 0 1 4 】

また、異なるサービスを提供する複数の異なるサービスプロバイダの提供するサービスを1つのユーザデバイスが受けようとする場合、ユーザデバイス側では、各サービスプロバイダが設定した独自の仕様、アプリケーションに従った設定を、個々のサービス毎に実行することが必要であった。また、サービスプロバイダ側でも、それぞれ独自にユーザ情報をユーザデバイスを介して受領し、独自に管理、審査を実行して自身の提供するサービスに対する許可または拒否等の判定を実行することが必要となっている。

【 0 0 1 5 】

例えば、ユーザデバイスが新たなサービスプロバイダの提供する新たなサービスを開始したい場合には、そのサービスプロバイダの要求する項目に従ったユーザデータ、端末データ等をサービスプロバイダに送信し、サービスプロバイダはユーザデバイスからのデータに基づいて、ユーザを登録しサービスを開始していた。

【 0 0 1 6 】

このように、サービス毎に独自のユーザ管理、アクセス制御を行なうことは、サービスプロバイダ、ユーザ双方にとって負担であり、また、双方のデバイスにおいて、様々な登録用のデータを格納、管理することが要求されることになり、デバイス自体の負担も増加することになる。

【 0 0 1 7 】

本発明は、このような点に鑑みてなされたものであり、様々なサービスプロバイダが提供するサービスへのユーザデバイスからのアクセスに対する制御をサービスプロバイダ個々が独自に実行することが要求されないアクセス制御システムおよびアクセス制御方法を実現することを目的とする。

【 0 0 1 8 】

【課題を解決するための手段】

本発明の第1の側面は、

公開鍵証明書発行局が認証対象に発行する公開鍵証明書を利用して公開鍵系暗号方式を使用したデータ転送を行なうデータ転送システムにおけるアクセス制御システムにおいて、

前記認証対象であり、サービスを提供するサービスプロバイダと、

前記認証対象であり、前記サービスプロバイダの提供するサービスを受領するサービス受領デバイスと、

前記サービス受領デバイスのアクセスが許可されたサービスプロバイダを識別可能なアクセス許可書を前記サービス受領デバイスに対して発行するアクセス制御サーバとを有し、

前記サービス提供プロバイダは、前記サービス受領デバイスからのアクセス要求に対するアクセス許可判定を、前記アクセス許可書に基づいて実行する構成であることを特徴とするアクセス制御システムにある。

【0019】

さらに、本発明のアクセス制御システムの一実施態様において、アクセス制御サーバ登録サーバを有し、前記アクセス制御サーバ登録サーバは、前記サービス受領デバイスからのアクセス許可書発行要求を受領して、前記アクセス制御サーバに対するアクセス許可書発行処理の実行要求を行なう構成であることを特徴とする。

【0020】

さらに、本発明のアクセス制御システムの一実施態様において、ユーザ端末によって利用可能なコンテンツまたはサービスの提供を可能とするコンテンツまたはサービスの流通インフラを提供または管理する機関であるシステムホルダを有し、前記システムホルダは、前記サービスプロバイダおよびサービス受領デバイスを管轄し、認証対象とした構成であることを特徴とする。

【0021】

さらに、本発明のアクセス制御システムの一実施態様において、前記アクセス制御サーバは、前記システムホルダ各々に対応して設けられ、前記システムホル

ダの管轄するサービスプロバイダの提供するサービスに関するアクセス許可書を発行する構成であることを特徴とする。

【 0 0 2 2 】

さらに、本発明のアクセス制御システムの一実施態様において、前記アクセス制御サーバは、前記システムホルダの複数に対して共通に設けられ、該複数のシステムホルダの管轄するサービスプロバイダの提供するサービスに関するアクセス許可書を発行する構成であることを特徴とする。

【 0 0 2 3 】

さらに、本発明のアクセス制御システムの一実施態様において、前記システムホルダを管轄するルート登録局を有し、前記ルート登録局は、前記システムホルダからの要求に基づいて該ルート登録局の管轄する認証対象の公開鍵証明書の発行要求を前記公開鍵証明書発行局に対して実行する構成であることを特徴とする。

【 0 0 2 4 】

さらに、本発明のアクセス制御システムの一実施態様において、前記アクセス制御サーバは、前記アクセス許可書を、サービスプロバイダ毎に独立に使用可能な態様で生成することを特徴とする。

【 0 0 2 5 】

さらに、本発明のアクセス制御システムの一実施態様において、前記アクセス制御サーバは、前記アクセス許可書を、複数のサービスプロバイダに共通に使用可能な態様で生成することを特徴とする。

【 0 0 2 6 】

さらに、本発明のアクセス制御システムの一実施態様において、前記アクセス制御サーバは、前記アクセス制御サーバの設定するアクセス制御サーバ設定固定フィールドと、前記サービスプロバイダの各々が設定するサービスプロバイダ設定オプションフィールドと、

前記アクセス制御サーバによる電子署名フィールドと、から成るフォーマットで、前記アクセス許可書を生成する構成であることを特徴とする。

【 0 0 2 7 】

さらに、本発明のアクセス制御システムの一実施態様において、前記サービスプロバイダ設定オプションフィールドには、サービス受領デバイス毎のアクセス可否を決定する識別データを含み、該識別データは、前記サービス受領デバイスのユーザに関する個人情報、ユーザID、ユーザデバイスID、またはアクセス許可識別フラグの少なくともいずれかを含む構成であることを特徴とする。

【0028】

さらに、本発明のアクセス制御システムの一実施態様において、前記サービスプロバイダ、前記サービス受領デバイス、前記アクセス制御サーバ間において、直接あるいは仲介手段を介して実行されるデータ転送は、データ転送相互間における相互認証処理が実行され、相互認証が成立したことを条件としたデータ転送として実行する構成であることを特徴とする。

【0029】

さらに、本発明のアクセス制御システムの一実施態様において、前記サービスプロバイダ、前記サービス受領デバイス、前記アクセス制御サーバ間において、直接あるいは仲介手段を介して実行される転送データはデータ送信側の電子署名が付加されたデータとして転送する構成であることを特徴とする。

【0030】

さらに、本発明のアクセス制御システムの一実施態様において、前記サービスプロバイダは、サービスを提供するデバイスであることを特徴とする。

【0031】

さらに、本発明のアクセス制御システムの一実施態様において、前記アクセス制御サーバは、前記アクセス許可書に設定されたアクセス許可を取り消すアクセス許可書の変更処理を実行する構成であることを特徴とする。

【0032】

さらに、本発明の第2の側面は、

公開鍵証明書発行局が認証対象に発行する公開鍵証明書を利用して公開鍵系暗号方式を使用したデータ転送を行なうデータ転送システムにおけるアクセス制御方法であり、

サービス提供プロバイダにおいて、サービス受領デバイスから、サービス制御

サーバの発行したアクセス許可書を受領するステップと、

前記アクセス許可書に基づいて、前記サービス受領デバイスのアクセス要求に対するアクセス許可判定を実行するステップと、

を有することを特徴とするアクセス制御方法にある。

【 0 0 3 3 】

さらに、本発明のアクセス制御方法の一実施態様において、アクセス制御サーバにおいて、サービス受領デバイスのアクセスが許可されたサービスプロバイダを識別可能なアクセス許可書をサービス受領デバイスに対して発行するアクセス許可書発行ステップとを含むことを特徴とする。

【 0 0 3 4 】

さらに、本発明のアクセス制御方法の一実施態様において、前記アクセス制御サーバ登録サーバにおいて、前記サービス受領デバイスからのアクセス許可書発行要求を受領して、前記アクセス制御サーバに対するアクセス許可書発行処理の実行要求を行なうステップを有することを特徴とする。

【 0 0 3 5 】

さらに、本発明のアクセス制御方法の一実施態様において、前記アクセス許可書発行ステップは、ユーザ端末によって利用可能なコンテンツまたはサービスの提供を可能とするコンテンツまたはサービスの流通インフラを提供または管理する機関であるシステムホルダの管轄するサービスプロバイダからの発行要求に基づいて実行されることを特徴とする。

【 0 0 3 6 】

さらに、本発明のアクセス制御方法の一実施態様において、前記アクセス許可書発行ステップは、サービスプロバイダ毎に独立に使用可能な態様で前記アクセス許可書を生成することを特徴とする。

【 0 0 3 7 】

さらに、本発明のアクセス制御方法の一実施態様において、前記アクセス許可書発行ステップは、複数のサービスプロバイダに共通に使用可能な態様で前記アクセス許可書を生成することを特徴とする。

【 0 0 3 8 】

さらに、本発明のアクセス制御方法の一実施態様において、前記アクセス許可書発行ステップは、前記アクセス制御サーバの設定するアクセス制御サーバ設定固定フィールドと、前記サービスプロバイダの各々が設定するサービスプロバイダ設定オプションフィールドと、前記アクセス制御サーバによる電子署名フィールドと、から成るフォーマットで生成することを特徴とする。

【 0 0 3 9 】

さらに、本発明のアクセス制御方法の一実施態様において、前記サービスプロバイダにおいて実行されるアクセス許可判定実行ステップは、前記アクセス許可書に含まれるサービス受領デバイス毎のアクセス可否を決定する識別データとしての前記サービス受領デバイスのユーザに関する個人情報、ユーザID、ユーザデバイスID、またはアクセス許可識別フラグの少なくともいずれかに基づいてアクセス許可の判定を実行することを特徴とする。

【 0 0 4 0 】

さらに、本発明のアクセス制御方法の一実施態様において、前記サービスプロバイダ、前記サービス受領デバイス、前記アクセス制御サーバ間において、直接あるいは仲介手段を介して実行されるデータ転送は、データ転送相互間における相互認証処理を実行し、相互認証が成立したことを条件としたデータ転送として実行することを特徴とする。

【 0 0 4 1 】

さらに、本発明のアクセス制御方法の一実施態様において、前記サービスプロバイダ、前記サービス受領デバイス、前記アクセス制御サーバ間において、直接あるいは仲介手段を介して実行される転送データにはデータ送信側の電子署名を付加することを特徴とする。

【 0 0 4 2 】

さらに、本発明のアクセス制御方法の一実施態様において、前記アクセス制御サーバにおいて、前記アクセス許可書に設定されたアクセス許可を取り消すアクセス許可書の変更処理を実行するアクセス許可書変更処理ステップを含むことを特徴とする。

【 0 0 4 3 】

さらに、本発明の第3の側面は、

公開鍵証明書発行局が認証対象に発行する公開鍵証明書を利用して公開鍵系暗号方式を使用したデータ転送を行なうデータ転送システムにおけるアクセス制御処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、

サービス提供プロバイダにおいて、サービス受領デバイスから、サービス制御サーバの発行したアクセス許可書を受領するステップと、

前記アクセス許可書に基づいて、前記サービス受領デバイスのアクセス要求に対するアクセス許可判定を実行するステップと、

を有することを特徴とするプログラム提供媒体にある。

【0044】

本発明の第3の側面に係るプログラム提供媒体は、例えば、様々なプログラム・コードを実行可能な汎用コンピュータ・システムに対して、コンピュータ・プログラムをコンピュータ可読な形式で提供する媒体である。媒体は、CDやFD、MOなどの記憶媒体、あるいは、ネットワークなどの伝送媒体など、その形態は特に限定されない。

【0045】

このようなプログラム提供媒体は、コンピュータ・システム上で所定のコンピュータ・プログラムの機能を実現するための、コンピュータ・プログラムと提供媒体との構造上又は機能上の協働的關係を定義したものである。換言すれば、該提供媒体を介してコンピュータ・プログラムをコンピュータ・システムにインストールすることによって、コンピュータ・システム上では協働的作用が発揮され、本発明の他の側面と同様の作用効果を得ることができるのである。

【0046】

本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。

【0047】

【発明の実施の形態】

以下、図面を参照しながら、本発明の実施の形態について詳細に説明する。

【0048】

【実施例】

[階層構成を持つデータ配信システム概要]

まず、図2を用いて、本発明のアクセス制御システムおよびアクセス制御方法を実行可能なデータ通信システムのシステム構成例を説明する。図2のシステムは、公開鍵系暗号を使用したデータ通信システム構成例である。

【0049】

図2において、ショップ206、端末207、ユーザデバイス208、ユーザの決済機関209が認証対象者、すなわち公開鍵暗号化方式によるデータ送受信を実行する主体となる。図2では、代表的な認証対象者としてショップ206、端末207、ユーザデバイス208、ユーザの決済機関209をそれぞれ1つずつ示しているが、これらは一般に多数存在し、また、これら以外にも様々な種類の認証対象者が存在することができる。

【0050】

各々の登録局(RA)の管轄下にある認証対象者のショップ206、端末207、ユーザデバイス208、ユーザの決済機関209は、登録局(サービスプロバイダRA)203、204、登録局(ペイメントRA)205に対して、自己の使用する公開鍵に対応する公開鍵証明書の発行を要求する。

【0051】

登録局(RA:Registration Authority)203、204、205は、各サービスにおける対象(サービスに参加するエンティティ、機器)を認証、あるいはそのサービスへの参加者の支払者を認証する(支払に対する保証)。また、登録局203、204、205は、各サービスにおける対象(サービスに参加するエンティティ、機器、ユーザ)の使用する公開鍵の公開鍵証明書発行要求を受領し、これをルート登録局(ルートRA)202を介して公開鍵証明書発行局(IA)201に転送する。ルート登録局(ルートRA)202は、認証済みの登録局203、204、205からの公開鍵証明書発行要求を受理する。すなわち、ルート登録局(ルートRA)202が公開鍵証明書発行要求を受領するのは、ルート登録局(ルートRA)202によって認証された登録局からの要求のみである

【0052】

図2において、例えば登録局（サービスプロバイダRA）203、204は音楽データ、画像データ、ゲームプログラム等のコンテンツ配信のサービス提供を実行するサービスプロバイダであり、登録局（ペイメントRA）205は、銀行等のユーザの決済機関209とデータ送受信を行ない、ユーザの電子マネーの決済処理を実行するクリアリングセンタである。これら、登録局（RA）についても図2に示すものは一例であり、この他にも様々なサービスを提供する各種の登録局（RA）が存在可能である。

【0053】

登録局（RA）は各サービス（システム）毎に存在し、その登録局（RA）を統括して認証するものとしてルートRA（Root Registration Authority）202が存在する。ルートRA（Root RA）202は次に述べるIAによって認証される。登録局（RA）203、204、205は、小規模なサービス主体であり、サービス提供者が独自のRAを持たない場合にはルートRA（Root RA）202が機能を代行する事ができる。

【0054】

図2に示すIA，201は公開鍵証明書発行局（IA：Issuer Authority）である。ルート登録局（ルートRA）202、または登録局（RA）203～205との間で相互認証を行い、ルートRA202、または登録局（RA）203～205から渡される公開鍵証明書発行要求主体である対象を識別する対象識別子（ID）、対象の公開鍵、その他の公開鍵証明書に書き込む情報を元に公開鍵証明書を作成して登録局（RA）203～205に配布する。

【0055】

公開鍵証明書発行局（IA）201に対して証明書発行を要求するルート登録局（ルートRA）202、または登録局（RA）203～205は、公開鍵証明書発行局から認証されていることが条件となる。

【0056】

また、公開鍵証明書発行局（IA）201は、ルート登録局（ルートRA）2

02、または登録局（RA）203～205の要求を受けて、公開鍵証明書の更新、無効化、削除あるいは対象者からの有効性確認に対する応答処理を行う。この公開鍵証明書発行局（IA：Issuer Authority）201は適切な法的機関の認定を受ける位置づけのものであり、その認可を持って認証されているものとする。

【0057】

〔システムホルダを構成要素としたデータ配信構成〕

次に、上述のルート登録局（ルートRA）と登録局（RA）との階層構成において、登録局（RA）をシステムホルダ（SH）として設定した構成例について説明する。

【0058】

システムホルダ（SH）は、例えばインターネット上で展開するインターネットショッピングマーケットを主催、管理する機関、携帯電話の通信インフラを提供する機関、ケーブルテレビのケーブル使用を管理する機関、電子マネー・カード発行主体等によって構成される。すなわち、システムホルダは、様々なコンテンツ、サービスを提供可能とするコンテンツまたはサービスの流通インフラを提供、管理する機関として定義される。

【0059】

図3にシステムホルダ301、コンテンツクリエイタ302、サービスプロバイダ303、ユーザ304の関係図を示し、図4にシステムホルダ、コンテンツクリエイタ、サービスプロバイダ、ユーザデバイスの具体例を示す。

【0060】

図3において、システムホルダ301は、コンテンツクリエイタ302および、サービスプロバイダ303、ユーザ（デバイス）304において利用可能なコンテンツまたはサービス流通インフラを提供する。コンテンツクリエイタ302および、サービスプロバイダ303は、システムホルダ301の提供するインフラを利用してコンテンツの提供あるいはサービスの提供を行なう。ユーザ（デバイス）304は、システムホルダ301の提供するインフラを利用してサービスプロバイダ303の提供するサービスを受ける。

【0061】

図4に、具体的なシステムホルダ、コンテンツクリエイタ、サービスプロバイダ、ユーザデバイスの例を示す。図4に示すように、例えば、システムホルダ（SH）が、インターネットショップマーケットを主催、管理する機関である場合、コンテンツクリエイタ（CC）は、インターネットショップマーケットに提供される商品を提供する。サービスプロバイダ（SP）は、提供された商品をインターネットショップにおいて販売するショップ（店）であり、ユーザデバイスは、インターネットショップを利用するPC等である。

【0062】

また、システムホルダ（SH）が、通信会社等、携帯電話通信インフラの提供機関である場合、コンテンツクリエイタ（CC）は、携帯電話の通信インフラを利用して提供可能なコンテンツ、商品を作成、製造する。サービスプロバイダ（SP）は、コンテンツクリエイタ（CC）から提供されるコンテンツ、商品を携帯電話の通信インフラを利用してユーザに対して販売、提供する。この場合のユーザデバイスは、携帯電話となる。

【0063】

また、システムホルダ（SH）が、ケーブルテレビのケーブル通信管理会社等、ケーブルテレビ通信インフラの提供機関である場合、コンテンツクリエイタ（CC）は、ケーブルテレビの通信インフラを利用して提供可能なコンテンツ、商品を作成、製造する。ケーブルテレビに提供される番組もコンテンツに含まれる。サービスプロバイダ（SP）は、コンテンツクリエイタ（CC）から提供されるコンテンツ、商品をケーブルテレビの通信インフラを利用してユーザに対して販売、提供する、例えば視聴者から直接、視聴料金を徴収するケーブルテレビ会社等である。

【0064】

また、システムホルダ（SH）が、電子マネーの発行機関等、電子マネー決済処理インフラの提供機関である場合、コンテンツクリエイタ（CC）は、電子マネーによって利用（購入）可能なコンテンツ、商品の提供機関であり、サービスプロバイダ（SP）は、コンテンツクリエイタ（CC）から提供されるコンテン

ツ、商品を電子マネーを利用可能なショップとして実現した販売店となる。この場合のユーザデバイスは、電子マネーを入力可能なICカード等になる。

【0065】

この他にも、様々なタイプのシステムホルダ（SH）があり、システムホルダに応じてコンテンツクリエイタ（CC）、サービスプロバイダ（SP）、ユーザデバイスが構成される。すなわち、システムホルダ（SH）は、コンテンツクリエイタ（CC）、サービスプロバイダ（SP）、ユーザデバイスによって利用可能なコンテンツ、サービスの提供を可能とするためのコンテンツまたはサービスの流通インフラを提供、管理する機関として定義される。

【0066】

ここでは、前述の登録局（RA）の機能をシステムホルダ（SH）が担う構成とすることにより、ユーザにとって利用し易いコンテンツまたはサービスの流通構成について説明する。

【0067】

まず、図5を用いて、前述の登録局（RA）の機能をシステムホルダ（SH）に付与しない形態での公開鍵暗号方式によるコンテンツまたはサービスの流通構成について説明する。

【0068】

図5に示すように、ユーザが利用可能なサービスは様々、存在するが、各々が独自の公開鍵暗号方式、すなわち独自の審査、独自の登録により特定のサービスにおいてのみ有効な独自の公開鍵証明書を発行して特定サービスの提供を行なっている。この従来型のサービス提供構成を示したのが図5である。図5では、サービスAを提供するグループ510と、サービスBを提供するグループ520を示している。

【0069】

サービスAを提供するグループ510には、サービスAの提供のために利用可能な公開鍵証明書発行局（IA-A）511、公開鍵証明書の利用を要求するサービスプロバイダ（SP）514、ユーザ（デバイス）515の登録管理を実行する登録局（RA-A）512が設置され、登録局512は、例えば公的な審査

機関 513 の審査に基づいて、サービスプロバイダ 514、ユーザ（デバイス）515 の登録を行ない、公開鍵証明書発行局（IA-A）511 に証明書の発行を要求し、サービスプロバイダ 514、ユーザ（デバイス）515 の管理を行なう。なお、公開鍵証明書発行局（IA-A）511 と登録局 512 によって認証局 A（CA-A）が構成される。

【0070】

サービス B を提供するグループ 520 には、サービス B の提供のために利用可能な公開鍵証明書発行局（IA-B）521、公開鍵証明書の利用を要求するサービスプロバイダ（SP）524、ユーザ（デバイス）525 の登録管理を実行する登録局（RA-B）522 が設置され、登録局 522 は、例えば公的な審査機関 523 の審査に基づいて、サービスプロバイダ 524、ユーザ（デバイス）525 の登録を行ない、公開鍵証明書発行局（IA-B）521 に証明書の発行を要求し、サービスプロバイダ 514、ユーザ（デバイス）525 の管理を行なう。なお、公開鍵証明書発行局（IA-B）521 と登録局 522 によって認証局 B（CA-B）が構成される。

【0071】

このような構成において、例えばサービス A の提供を受けるために、登録局（RA-A）512 を介して登録を行い、サービス A で適用可能な公開鍵証明書の発行を受けているユーザ 515 が、サービス B のサービスを受けようとした場合は、発行済みの公開鍵証明書は使用できない。ユーザ 515 が、サービス B のサービスを受けるためには、サービス B を管轄する登録局（RA-B）522 を介して新たな登録手続きを行なって新たな公開鍵証明書の発行を受けることが必須となる。

【0072】

これを解決するには、図 5 に示す公開鍵証明書発行局と登録局によって構成される認証局（CA）相互間で認証する構成としたり、あるいは認証局（CA）を階層構造とすることが考えられるが、認証局（CA）の処理負担の増加、認証局（CA）構造の複雑化を招くという欠点がある。一方、ユーザが複数のサービスを受けるためにサービス毎の複数の公開鍵証明書をデバイス中に格納する構成と

すると、ユーザデバイスの記憶領域を公開鍵証明書記憶のために多く使用することになる。このような構成は、例えばユーザデバイスがICカードのような限定されたメモリ領域を有するデバイスにおいては問題である。

【0073】

また、図5のユーザデバイス515とユーザデバイス525との相互間で、例えばオフラインでの相互認証を行なおうとした場合、それぞれの管轄認証局(CA)が異なっているため認証処理が実行できないことになる。相互認証を有効に実行するためには、デバイス自身管轄の認証局の公開鍵と、相手デバイスの管轄の認証局の公開鍵の層法をデバイスに格納することが必要となり、様々な相手デバイスとの認証が必要となる場合には、格納公開鍵の数もさらに増加することになる。

【0074】

このように、サービス毎に独立した管理を行なう図5の構成では、様々な問題が発生する。この問題を解決するのが図6に示すシステムホルダ(SH)をルート登録局(ルートRA)の下に階層に設定した構成である。

【0075】

図6の構成について説明する。図6の構成は、先の図5の構成に対応した構成であり、図の左側がサービスA、右側がサービスBを提供するサービスプロバイダ集合が含まれる。サービスプロバイダ604は、サービスAの提供主体であり、サービスプロバイダ607は、サービスBの提供主体である。

【0076】

サービスプロバイダ604、ユーザ(デバイス)605、サービスプロバイダ607、ユーザ(デバイス)608が認証対象者、すなわち公開鍵暗号化方式によるデータ送受信を実行する主体となる。図6では、2つのサービスA、Bについての構成を示しているが、サービスは一般に多数存在することができる。

【0077】

システムホルダA、603は、前述の登録局(RA)としての役割、機能を実行する。管轄下にある認証対象者のサービスプロバイダ604、ユーザ(デバイス)605は、システムホルダA、603に対して、自己の使用する公開鍵に対

応する公開鍵証明書の発行を要求する。システムホルダB, 606は、管轄下にある認証対象者のサービスプロバイダ607、ユーザ（デバイス）608からの公開鍵証明書の発行要求を受領する。

【0078】

システムホルダA, 603、システムホルダB, 606は、各サービスにおける対象（サービスに参加するエンティティ、機器）を認証する。また、システムホルダA, 603、システムホルダB, 606は、各サービスにおける対象（サービスに参加するエンティティ、機器、ユーザ）の使用する公開鍵の公開鍵証明書発行要求を受領し、これをルート登録局（ルートRA）602を介して、あるいは直接、公開鍵証明書発行局（IA）601に転送する。

【0079】

ルート登録局（ルートRA）602を介する処理の場合、ルート登録局（ルートRA）602は、予め実行された認証が成立済みのシステムホルダA, 603、システムホルダB, 606から公開鍵証明書発行要求を受領する。すなわち、ルート登録局（ルートRA）602が公開鍵証明書発行要求を受領するのは、ルート登録局（ルートRA）602によって認証されたシステムホルダA, 603、システムホルダB, 606からの要求である。なお、システムホルダA, 603、システムホルダB, 606と直接、公開鍵証明書発行局（IA）601とのデータ通信を行なう場合も認証が成立したことが条件とされる。

【0080】

図6において、サービスプロバイダ604、サービスプロバイダ607は、例えば音楽データ、画像データ、ゲームプログラム等のコンテンツ配信のサービス提供を実行するサービスプロバイダであり、例えば、先に図4を用いて説明した各種のサービスを提供するサービス提供主体によって構成される。

【0081】

システムホルダA, 603、システムホルダB, 606は、サービスプロバイダ604、サービスプロバイダ607の提供するサービスを実現するインフラを管理する機関であり、図4を用いて説明したように、携帯電話通信インフラ提供者、電子マネー・カード発行機関等によって構成される。

【0082】

本構成の特徴は、コンテンツ提供、サービス提供を実現するインフラを提供または管理する機関であるシステムホルダが公開鍵証明書による認証、データ通信を実行するサービスプロバイダ、ユーザデバイスの公開鍵証明書発行手続き仲介、登録管理を行なう点である。システムホルダは、コンテンツ提供、サービス提供を実現するインフラを提供または管理する機関であるので、そのインフラを利用するユーザ、あるいはサービスプロバイダの管理を行なっている場合が多く、管理用のデータベースを備えている構成であることが多い。このような管理データベースを利用して公開鍵証明書発行先の管理を併せて行なうことで効率的なユーザ、あるいはサービスプロバイダ管理が実行可能となる。

【0083】

また、例えば新たな通信インフラが構築され、新たなシステムホルダが出現した場合に、その新規システムホルダを既存のルート登録局（ルートRA）、公開鍵証明書発行局（IA）の管轄下に設定することで、容易に新規のインフラを利用した公開鍵証明書発行構成が実現され、新たなインフラを利用したサービスの提供がいち早く実現できる。

【0084】

ユーザデバイスは、1つの公開鍵証明書を格納するのみで、様々なサービスを利用可能となる。すなわち、図6の構成では、1つのルート登録局（ルートRA）、公開鍵証明書発行局（IA）が様々なシステムホルダ、サービスプロバイタに対応して設定されているので、ユーザデバイスは1つの公開鍵証明書を持つことにより、異なるサービスにおいて利用可能となる。また、異なるシステムホルダの管轄下のユーザデバイス相互間においても、1つの共通する公開鍵証明書発行局（IA）の発行する公開鍵を用いることにより、相互認証が可能となる。

【0085】

〔アクセス制御サーバを構成要素としたデータ配信構成〕

次に、上述のシステムホルダを用いた構成において、さらに、アクセス制御サーバを構成要素とした例について説明する。図7にアクセス制御サーバを設けた公開鍵証明書を用了データ配信システムの構成ブロック図を示す。

【0086】

図7の構成について説明する。公開鍵証明書を発行する公開鍵証明書発行局（IA）701、1以上のシステムホルダを管轄するルートRA702、1以上のサービスプロバイダ、デバイスを管轄するシステムホルダ703、750、ユーザデバイスに対してコンテンツの配信等、様々なサービスの提供を実行するサービスプロバイダ705、706、707、サービスプロバイダからのサービス提供を受けるユーザデバイス708、709を有し、さらに、本構成ではアクセス制御サーバ710、アクセス制御サーバ登録サーバ720を有する。本構成において、サービスプロバイダ、ユーザデバイスが主たるデータ送受信者、すなわち公開鍵暗号化方式によるデータ送受信を実行する主体となる。

【0087】

図7の構成では、アクセス制御サーバ710は、1つのシステムホルダ703に対応して設定されており、システムホルダの703管轄するサービスプロバイダ705～707に対するデバイス708、709からのアクセスの可否を決定するためのアクセス許可書発行処理を実行する。すなわち、ユーザデバイス708、709に対してアクセスの認められたサービスプロバイダを設定したアクセス許可書を発行する。ユーザデバイス708、709は、サービスプロバイダ705～707に対するアクセス時にアクセス制御サーバ710の発行したアクセス許可書をサービスプロバイダ705～707に提示する。サービスプロバイダは、ユーザデバイス708、709から受領したアクセス許可書に基づいて、アクセスの可否を判定する。アクセス許可書については後段で詳細に説明する。

【0088】

また、アクセス制御サーバ登録サーバ720は、システムホルダ703の管轄するサービスプロバイダ705～707とのデータ通信を実行し、ユーザデバイス708、709からのアクセス許可書発行要求をサービスプロバイダ705～707を介して受信し、受信したユーザデバイス708、709からのアクセス許可書発行要求に基づいてアクセス制御サーバ710にアクセス許可書の発行依頼を行なう。

【0089】

なお、図7に示す各エンティティ（ルートRA，SH，SP，ユーザデバイス）は公開鍵証明書（IA）の発行した公開鍵証明書を有し、各エンティティ間のデータ通信は、公開鍵ベースでの認証処理を実行して、必要に応じてセッション鍵を生成してセッション鍵での暗号化を実行してデータ通信を実行する。

【0090】

図7の構成は、アクセス制御サーバ710、アクセス制御サーバ登録サーバ720は、1つのシステムホルダ703に対応して設定された構成であるが、アクセス制御サーバ、アクセス制御サーバ登録サーバを複数のシステムホルダ共通に利用可能とする構成としてもよい。

【0091】

複数のシステムホルダに共通に利用可能なアクセス制御サーバ、アクセス制御サーバ登録サーバを有する構成を図8に示す。図8において、アクセス制御サーバ810、アクセス制御サーバ登録サーバ820は、複数のシステムホルダ703，750に共通に利用可能な構成である。システムホルダ703管轄下にあるサービスプロバイダ705～707、ユーザデバイス708，709、さらにシステムホルダ750の管轄下にあるサービスプロバイダ751、ユーザデバイス752は、すべてアクセス制御サーバ810、アクセス制御サーバ登録サーバ820によって管理され、アクセス制御サーバ810の発行するアクセス許可書を利用する。

【0092】

[アクセス許可書]

次に、図7、図8に示すアクセス制御サーバの発行するアクセス許可書について説明する。アクセス許可書の発行形態は大きく分けて2種類ある。第1の方式は、1つのサービスプロバイダに対してのみ有効なサービスプロバイダ固有のアクセス許可書（方式A）であり、第2の方式は、複数のサービスプロバイダに対して共通に有効なアクセス許可書（方式B）である。

【0093】

これら2つの方式の例を図9に示す。方式Aは、サービスプロバイダ（SP）毎に、それぞれサービスプロバイダの要求するデータ項目を含む様式で作成され

、1つのアクセス許可書が1つのサービスプロバイダにのみ有効な方式である。一方、方式Bは、複数のサービスプロバイダに共通に利用可能な方式であり、各サービスプロバイダの要求するデータ項目をそれぞれ含む様式で作成される。方式Aの場合、ユーザデバイスは、アクセスの実行を行なうサービスプロバイダ個々のアクセス許可書を保有することになる。一方、方式Bの場合は、1つのアクセス許可書のみを格納するのみで、複数のサービスプロバイダに対して対処可能となる。

【0094】

図10に、方式Bの場合のアクセス許可書のサンプルを示す。アクセス許可書は、アクセス制御サーバ（ACS）が設定する固定フィールドと、各サービスプロバイダ（SP）が設定するオプションフィールド、さらにアクセス制御サーバ（ACS）による署名フィールドに区分される。

【0095】

固定フィールドには、アクセス許可書のシリアル番号、有効期限、アクセス許可書の発行対象者の公開鍵証明書（PKC）のシリアル番号、アクセス許可書のフォーマットのバージョン番号、アクセス許可書発行者（この場合はACS）の発行者識別名、さらに、アクセス許可書に付加された署名のアルゴリズム（例えば楕円曲線暗号方式、あるいはRSA方式等）を識別する署名方式が含まれる。

【0096】

シリアル番号は、アクセス許可書発行者（この場合はACS）によって設定されるアクセス許可書のシリアルナンバである。

有効期限(validity)は、証明書の有効期限である開始日時、終了日時が記録される。

公開鍵証明書（PKC）のシリアル番号は、このアクセス許可書を使用するユーザデバイスが保有する公開鍵証明書のシリアル番号が記録される。

バージョン番号は、アクセス許可書のフォーマットのバージョンを示す。

発行者識別名は、アクセス許可書の発行者、すなわちアクセス制御サーバ（ACS）の名称が識別可能な形式（Distinguished Name）で記録されるフィールドである。

署名方式は、アクセス許可書に対する署名の署名アルゴリズムとそのパラメータを記録するフィールドである。なお、署名アルゴリズムとしては、楕円曲線暗号およびRSAがあり、楕円曲線暗号が適用されている場合はパラメータおよび鍵長が記録され、RSAが適用されている場合には鍵長が記録される。

【0097】

オプションフィールドは、各サービスプロバイダ（SP）が独自に設定可能なフィールドであり、それぞれのサービスプロバイダの識別名、データサイズ、内容によって構成されるサービスプロバイダ単位のフィールドによって構成される。内容の具体例については図11で説明する。さらに、オプションフィールドの全体のデータサイズが記録される。

【0098】

署名フィールドは、アクセス許可書発行者（この場合はACS）の署名がなされるフィールドである。

【0099】

図10に示すオプションフィールド中の、サービスプロバイダによって設定される「内容」のフィールド構成例を図11に示す。

【0100】

図11の方式イ）は、ユーザ情報を「内容」として格納した例である。例えば、性別、年齢、役職等の様々なユーザ情報を格納する。これらのユーザ情報は多くの場合、プライベートな秘密情報を含み、サービスプロバイダの固有秘密鍵を用いて暗号化されて格納される。この場合、暗号鍵バージョンが併せて記録され、サービスプロバイダは、自己の所有する秘密鍵で、必要に応じてユーザ情報を復号する。

【0101】

図11の方式ロ）は、「内容」としてユーザIDのみを格納する構成であり、サービスプロバイダは、ユーザIDに基づいて自身で保有するユーザ情報データベースにアクセス可能なリンクを形成して、必要なユーザ情報を取得可能とした構成である。本方式は、ユーザ情報をサービスプロバイダの保有するデータベースで一元管理可能として、重複したデータをアクセス許可書に格納する必要を排

除したものであり、個人情報の漏洩等の問題発生の可能性を押さえたセキュリティの高い構成である。

【0102】

図11の方式ハ)は、「内容」としてユーザに対してアクセスを許可したか否かを示す情報のみを格納する構成であり、サービスプロバイダは、例えばユーザに対してアクセスを許可した場合は「1」、しない場合は「0」を設定する。本構成は、ユーザの個人情報によらず、ユーザ登録を行なったか否かのみに基づいてアクセス許可を設定する構成において特に有効である。また、本構成は、必要なデータ量が極めて少ないのでアクセス許可書のデータ量を削減できる。さらに、複数のサービスプロバイダに対して、SP1:0, SP2:1, …SPn, 0等、一括したアクセス認否用のビットを割り当てる構成とすることにより、さらにデータ量を削減できる。

【0103】

【電子署名および認証処理】

次に、本発明のアクセス制御システムにおけるアクセス許可書の発行処理および利用において、各エンティティで実行される電子署名生成処理、検証処理、さらに認証処理の概要を説明する。電子署名および相互認証処理について説明した後に、本発明のアクセス許可書を利用した具体的処理の詳細を説明する。

【0104】

(電子署名)

公開鍵暗号方式を用いた電子署名の生成方法を図12を用いて説明する。図12に示す処理は、ECDSA (Elliptic Curve Digital Signature Algorithm)、IEEE P1363/D3)を用いた電子署名データの生成処理フローである。なお、ここでは公開鍵暗号として楕円曲線暗号 (Elliptic Curve Cryptography (以下、ECCと呼ぶ))を用いた例を説明する。なお、本発明のデータ処理装置においては、楕円曲線暗号以外にも、同様の公開鍵暗号方式における、例えばRSA暗号 (Rivest, Shamir, Adleman) など (ANSI X9.31))を用いることも可能である。

【0105】

図12の各ステップについて説明する。ステップS1において、 p を標数、 a 、 b を楕円曲線の係数（楕円曲線： $y^2 = x^3 + ax + b$ ）、 G を楕円曲線上のベースポイント、 r を G の位数、 K_s を秘密鍵（ $0 < K_s < r$ ）とする。ステップS2において、メッセージ M のハッシュ値を計算し、 $f = \text{Hash}(M)$ とする。

【0106】

ここで、ハッシュ関数を用いてハッシュ値を求める方法を説明する。ハッシュ関数とは、メッセージを入力とし、これを所定のビット長のデータに圧縮し、ハッシュ値として出力する関数である。ハッシュ関数は、ハッシュ値（出力）から入力を予測することが難しく、ハッシュ関数に入力されたデータの1ビットが変化したとき、ハッシュ値の多くのビットが変化し、また、同一のハッシュ値を持つ異なる入力データを探し出すことが困難である特徴を有する。ハッシュ関数としては、MD4、MD5、SHA-1などが用いられる場合もあるし、DES-CBCが用いられる場合もある。この場合は、最終出力値となるMAC（チェック値：ICVに相当する）がハッシュ値となる。

【0107】

続けて、ステップS3で、乱数 u （ $0 < u < r$ ）を生成し、ステップS4でベースポイントを u 倍した座標 $V(X_v, Y_v)$ を計算する。なお、楕円曲線上の加算、2倍算は次のように定義されている。

【0108】

【数1】

$P=(X_a, Y_a), Q=(X_b, Y_b), R=(X_c, Y_c)=P+Q$ とすると、

$P \neq Q$ の時（加算）、

$$X_c = \lambda^2 - X_a - X_b$$

$$Y_c = \lambda \times (X_a - X_c) - Y_a$$

$$\lambda = (Y_b - Y_a) / (X_b - X_a)$$

$P=Q$ の時（2倍算）、

$$X_c = \lambda^2 - 2X_a$$

$$Y_c = \lambda \times (X_a - X_c) - Y_a$$

$$\lambda = (3(X_a)^2 + a) / (2Y_a)$$

【0109】

これらを用いて点 G の u 倍を計算する（速度は遅いが、最もわかりやすい演算方法として次のように行う。 G 、 $2 \times G$ 、 $4 \times G \cdots$ を計算し、 u を 2 進数展開して 1 が立っているところに対応する $2^i \times G$ (G を i 回 2 倍算した値 (i は u の LSB から数えた時のビット位置)) を加算する。

【0110】

ステップ S5 で、 $c = Xv \bmod r$ を計算し、ステップ S6 でこの値が 0 になるかどうか判定し、0 でなければステップ S7 で $d = [(f + cKs) / u] \bmod r$ を計算し、ステップ S8 で d が 0 であるかどうか判定し、 d が 0 でなければ、ステップ S9 で c および d を電子署名データとして出力する。仮に、 r を 160 ビット長の長さであると仮定すると、電子署名データは 320 ビット長となる。

【0111】

ステップ S6 において、 c が 0 であった場合、ステップ S3 に戻って新たな乱数を生成し直す。同様に、ステップ S8 で d が 0 であった場合も、ステップ S3 に戻って乱数を生成し直す。

【0112】

次に、公開鍵暗号方式を用いた電子署名の検証方法を、図 13 を用いて説明する。ステップ S11 で、 M をメッセージ、 p を標数、 a 、 b を楕円曲線の係数（楕円曲線： $y^2 = x^3 + ax + b$ ）、 G を楕円曲線上のベースポイント、 r を G の位数、 G および $Ks \times G$ を公開鍵 ($0 < Ks < r$) とする。ステップ S12 で電子署名データ c および d が $0 < c < r$ 、 $0 < d < r$ を満たすか検証する。これを満たしていた場合、ステップ S13 で、メッセージ M のハッシュ値を計算し、 $f = Hash(M)$ とする。次に、ステップ S14 で $h = 1/d \bmod r$ を計算し、ステップ S15 で $h1 = fh \bmod r$ 、 $h2 = ch \bmod r$ を計算する。

【0113】

ステップ S16 において、既に計算した $h1$ および $h2$ を使い、点 $P = (Xp, Yp) = h1 \times G + h2 \cdot Ks \times G$ を計算する。電子署名検証者は、公開鍵 G および $Ks \times G$ を知っているのので、図 12 のステップ S4 と同様に楕円曲線上の

点のスカラ倍の計算ができる。そして、ステップS17で点Pが無限遠点かどうか判定し、無限遠点でなければステップS18に進む（実際には、無限遠点の判定はステップS16でできてしまう。つまり、 $P = (X, Y)$ 、 $Q = (X, -Y)$ の加算を行うと、 λ が計算できず、 $P + Q$ が無限遠点であることが判明している）。ステップS18で $X_p \bmod r$ を計算し、電子署名データ c と比較する。最後に、この値が一致していた場合、ステップS19に進み、電子署名が正しいと判定する。

【0114】

電子署名が正しいと判定された場合、データは改竄されておらず、公開鍵に対応した秘密鍵を保持する者が電子署名を生成したことがわかる。

【0115】

ステップS12において、電子署名データ c または d が、 $0 < c < r$ 、 $0 < d < r$ を満たさなかった場合、ステップS20に進む。また、ステップS17において、点Pが無限遠点であった場合もステップS20に進む。さらにまた、ステップS18において、 $X_p \bmod r$ の値が、電子署名データ c と一致していなかった場合にもステップS20に進む。

【0116】

ステップS20において、電子署名が正しくないと判定された場合、データは改竄されているか、公開鍵に対応した秘密鍵を保持する者が電子署名を生成したのではないことがわかる。

【0117】

(相互認証処理)

データ送受信を実行する2つの手段間では、相互に相手が正しいデータ通信者であるか否かを確認して、その後に必要なデータ転送を行なうことが行われる。相手が正しいデータ通信者であるか否かの確認処理が相互認証処理である。相互認証処理時にセッション鍵の生成を実行して、生成したセッション鍵を共有鍵として暗号化処理を実行してデータ送信を行なう構成が1つの好ましいデータ転送方式である。

【0118】

共通鍵暗号方式を用いた相互認証方法を、図14を用いて説明する。図14において、共通鍵暗号方式としてDESを用いているが、同様な共通鍵暗号方式であればいずれでもよい。

【0119】

まず、Bが64ビットの乱数R_bを生成し、R_bおよび自己のIDであるID(b)をAに送信する。これを受信したAは、新たに64ビットの乱数R_aを生成し、R_a、R_b、ID(b)の順に、DESのCBCモードで鍵K_{a b}を用いてデータを暗号化し、Bに返送する。

【0120】

これを受信したBは、受信データを鍵K_{a b}で復号化する。受信データの復号化方法は、まず、暗号文E₁を鍵K_{a b}で復号化し、乱数R_aを得る。次に、暗号文E₂を鍵K_{a b}で復号化し、その結果とE₁を排他的論理和し、R_bを得る。最後に、暗号文E₃を鍵K_{a b}で復号化し、その結果とE₂を排他的論理和し、ID(b)を得る。こうして得られたR_a、R_b、ID(b)の内、R_bおよびID(b)が、Bが送信したものと一致するか検証する。この検証に通った場合、BはAを正当なものとして認証する。

【0121】

次にBは、認証後に使用するセッション鍵 (Session Key (以下、K_{s e s}とする)) を生成する (生成方法は、乱数を用いる)。そして、R_b、R_a、K_{s e s}の順に、DESのCBCモードで鍵K_{a b}を用いて暗号化し、Aに返送する。

【0122】

これを受信したAは、受信データを鍵K_{a b}で復号化する。受信データの復号化方法は、Bの復号化処理と同様であるので、ここでは詳細を省略する。こうして得られたR_b、R_a、K_{s e s}の内、R_bおよびR_aが、Aが送信したものと一致するか検証する。この検証に通った場合、AはBを正当なものとして認証する。互いに相手を認証した後には、セッション鍵K_{s e s}は、認証後の秘密通信のための共通鍵として利用される。

【0123】

なお、受信データの検証の際に、不正、不一致が見つかった場合には、相互認証が失敗したものとして処理を中断する。

【0124】

次に、公開鍵暗号方式である160ビット長の楕円曲線暗号を用いた相互認証方法を、図15を用いて説明する。図15において、公開鍵暗号方式としてECCを用いているが、前述のように同様な公開鍵暗号方式であればいずれでもよい。また、鍵サイズも160ビットでなくてもよい。図15において、まずBが、64ビットの乱数 R_b を生成し、Aに送信する。これを受信したAは、新たに64ビットの乱数 R_a および標数 p より小さい乱数 A_k を生成する。そして、ベースポイント G を A_k 倍した点 $A_v = A_k \times G$ を求め、 R_a 、 R_b 、 A_v （X座標とY座標）に対する電子署名 $A.Sig$ を生成し、Aの公開鍵証明書とともにBに返送する。ここで、 R_a および R_b はそれぞれ64ビット、 A_v のX座標とY座標がそれぞれ160ビットであるので、合計448ビットに対する電子署名を生成する。電子署名の生成方法は図12で説明したので、その詳細は省略する。

【0125】

公開鍵証明書を利用する際には、利用者は自己が保持する公開鍵証明書発行局（IA）の公開鍵を用い、当該公開鍵証明書の電子署名を検証し、電子署名の検証に成功した後に公開鍵証明書から公開鍵を取り出し、当該公開鍵を利用する。従って、公開鍵証明書を利用する全ての利用者は、共通の公開鍵証明書発行局（IA）の公開鍵を保持している必要がある。なお、電子署名の検証方法については、図13で説明したのでその詳細は省略する。

【0126】

図15に戻って説明を続ける。Aの公開鍵証明書、 R_a 、 R_b 、 A_v 、電子署名 $A.Sig$ を受信したBは、Aが送信してきた R_b が、Bが生成したものと一致するか検証する。その結果、一致していた場合には、Aの公開鍵証明書内の電子署名を認証局の公開鍵で検証し、Aの公開鍵を取り出す。そして、取り出したAの公開鍵を用い電子署名 $A.Sig$ を検証する。電子署名の検証方法は図13で説明したので、その詳細は省略する。電子署名の検証に成功した後、BはAを正当なものとして認証する。

【0127】

次に、Bは、標数 p より小さい乱数 B_k を生成する。そして、ベースポイント G を B_k 倍した点 $B_v = B_k \times G$ を求め、 R_b 、 R_a 、 B_v （X座標とY座標）に対する電子署名 $B.Sig$ を生成し、Bの公開鍵証明書とともにAに返送する。

【0128】

Bの公開鍵証明書、 R_b 、 R_a 、 A_v 、電子署名 $B.Sig$ を受信したAは、Bが送信してきた R_a が、Aが生成したものと一致するか検証する。その結果、一致していた場合には、Bの公開鍵証明書内の電子署名を認証局の公開鍵で検証し、Bの公開鍵を取り出す。そして、取り出したBの公開鍵を用い電子署名 $B.Sig$ を検証する。電子署名の検証に成功した後、AはBを正当なものとして認証する。

【0129】

両者が認証に成功した場合には、Bは $B_k \times A_v$ （ B_k は乱数だが、 A_v は楕円曲線上の点であるため、楕円曲線上の点のスカラー倍計算が必要）を計算し、Aは $A_k \times B_v$ を計算し、これら点のX座標の下位64ビットをセッション鍵として以降の通信に使用する（共通鍵暗号を64ビット鍵長の共通鍵暗号とした場合）。もちろん、Y座標からセッション鍵を生成してもよいし、下位64ビットでなくてもよい。なお、相互認証後の秘密通信においては、送信データはセッション鍵で暗号化されるだけでなく、電子署名も付されることがある。

【0130】

電子署名の検証や受信データの検証の際に、不正、不一致が見つかった場合には、相互認証が失敗したものとして処理を中断する。

【0131】

このような相互認証処理において、生成したセッション鍵を用いて、送信データを暗号化して、相互にデータ通信を実行する。

【0132】

[アクセス許可書の発行および利用]

(使用する用語の説明)

次に、アクセス許可書の発行処理および利用における処理について、順次説明する。なお、以下の説明において使用される用語についての説明を図16に示す。これらについて簡単に説明する。鍵をKとして表記し、サフィックスとして公開鍵はP、秘密鍵はSを付加し、さらに所有者識別子（例えばa）を付加する。相互認証の際に生成され、暗号化、復号化処理に適用されるセッション鍵をK_sとする。Aが発行したBの公開鍵証明書をA<>とする。データの暗号化は、例えばセッション鍵K_sでデータ（data）を暗号化した場合は、E_{K_s}（data）として示す。同様の復号は、D_{K_s}（data）として示す。署名処理は、例えばデータ（data）をAの秘密鍵K_{sa}で署名した場合は、{data}Sig・K_{sa}として示す。また、署名付き暗号化データは、例えばデータ（data）をAの秘密鍵K_{sa}で署名して生成される（data||署名）をセッション鍵K_sで暗号化した場合は、E_{K_s}（{data}Sig・K_{sa}）で示す。

【0133】

（デバイスに対する1枚目のアクセス許可書の発行処理）

次に、本発明のアクセス制御システムにおいて、ユーザデバイスが、サービスプロバイダのアクセス許可を取得するための処理として、最初のアクセス許可書を取得する処理シーケンスについて説明する。

【0134】

この場合の処理順序を、各エンティティ間でのデータの送受信順序に従って示した図を図17に示す。図17に示す番号（n）に従って、最初のアクセス許可書を取得するための処理が進行する。以下、各処理について説明する。

【0135】

まず、（1）の処理は、デバイス1705がサービスプロバイダ（SP11）1703のサービスを受けるための許可書を取得するため、サービスプロバイダ（SP11）1703求めるデータ、例えばユーザデバイスIDと、年齢等の各種のユーザ情報、デバイス情報を生成してサービスプロバイダに送信する。なお、データ送信前に、デバイス1705とサービスプロバイダ（SP11）1703間においては相互認証が実行され、セッション鍵E_{K_{s1}}が生成されている。（1）の処理における送信データは、ユーザデバイスID（UDID）と、その他

サービスプロバイダ1703の求める情報(data)を含み、これらにユーザデバイス1705の秘密鍵 K_{SUD} による署名が実行され、さらに、セッション鍵 E_{Ks1} を用いて暗号化処理が実行されたデータ： $E_{Ks1}(\{UDID, data\} \text{Sig} \cdot K_{SUD})$ となる。

【0136】

サービスプロバイダ(SP11)1703は、ユーザデバイス1705から受信した暗号化データをセッション鍵 E_{Ks1} で復号して、さらに署名検証を行ない、データ内容を審査して、サービスプロバイダ(SP11)1703の求める審査基準を満たすものである場合は、(2)の処理、すなわち、アクセス制御サーバ登録サーバ(RACS1)1702に対してアクセス許可書の発行依頼を行なう。

【0137】

この(2)の処理において、サービスプロバイダ(SP11)1703は、前述の図10を用いて説明したアクセス許可書におけるオプションフィールドの記載事項をアクセス制御サーバ登録サーバ(RACS1)1702に対して送信する。この場合、図12の各態様のいずれかに従った「内容」データを含むものとなる。例えば図12の方式イ)の場合は、サービスプロバイダ1703は、ユーザ情報を生成して必要に応じてサービスプロバイダ1703の鍵を用いて暗号化して送信データを生成する。図12の方式ロ)の場合はユーザIDのみ、図12の方式ハ)の場合はアクセス許可書の発行要求を行なうのみでよい。サービスプロバイダ(SP11)1703の生成したデータを(data2)とし、サービスプロバイダ(SP11)1703とアクセス制御サーバ登録サーバ(RACS1)1702間における相互認証処理の際に生成したセッション鍵 E_{Ks2} とすると、(2)の処理で送信されるデータは、 $E_{Ks2}(\{SPID, data2\} \text{Sig} \cdot K_{SSP})$ となる。

【0138】

アクセス制御サーバ登録サーバ(RACS1)1702が上記データをサービスプロバイダ(SP11)1703から受信すると、受信データに基づいてアクセス制御サーバ登録サーバ(RACS1)1702は、アクセス制御サーバ(A

CS1) 1701にアクセス許可書の発行要求を行なう((3)の処理)。

【0139】

次に、アクセス制御サーバ(ACS1) 1701は、要求データに基づいてアクセス許可書(ACPMS)を生成し、アクセス制御サーバ(ACS1) 1701の署名を実行したデータ： $\{ACPMS\} Sig \cdot K_{SACS1}$ をアクセス制御サーバ登録サーバ(RACS1) 1702に送信する((4)の処理)。なお、アクセス制御サーバ(ACS1) 1701とアクセス制御サーバ登録サーバ(RACS1) 1702とのデータ通信は、専用線のように外部からの割込みが排除されるセキュアな通信構成とした場合は、特に暗号化しないデータとして送受信する構成としてよい。通信ラインのセキュリティが不確実である場合は、上記の他のエンティティ間の通信と同様セッション鍵による暗号化処理を実行してデータ送受信を実行する。

【0140】

次に、アクセス制御サーバ登録サーバ(RACS1) 1702は、アクセス制御サーバ(ACS1) 1701からの受信データの署名検証処理を実行して、自分の署名を付加し、さらにセッション鍵で暗号化したデータ： $E_{Ks5}(\{ACPMS\} Sig \cdot K_{SACS1}) K_{SRACS1}$ をサービスプロバイダ(SP11) 1703に送信する((5)の処理)。

【0141】

次に、サービスプロバイダ(SP11) 1703は、アクセス制御サーバ登録サーバ(RACS1) 1702からの受信データの署名検証処理を実行して、自分の署名を付加し、さらにセッション鍵で暗号化したデータ： $E_{Ks6}(\{ACPMS\} Sig \cdot K_{SACS1}) K_{SRACS1}) K_{SSP}$ をユーザデバイス1705に送信する((6)の処理)。

【0142】

ユーザデバイス1705は、セッション鍵 E_{Ks4} での復号処理の後、署名検証を実行し、アクセス許可書(ACPMS)を自身のセキュアモジュールに格納する((7)の処理)。なお、格納の際には、自身の保存鍵 K_{str} を用いて暗号化処理を行なって保存することが望ましい。

【0143】

(デバイスにすでにアクセス許可書がある場合の新たなアクセス許可書の発行処理)

次に、すでにユーザデバイスがあるサービスプロバイダのアクセス許可書を有しており、新たに他のサービスプロバイダのアクセス許可書を取得する場合の処理について図18を用いて説明する。

【0144】

図18に示すユーザデバイス1705は、すでにサービスプロバイダ(SP11)1703のアクセス許可書を有しており、新たにサービスプロバイダ(SP12)1704のアクセス許可書を取得する。まず、ユーザデバイス1705は、サービスプロバイダ(SP12)1704求めるデータ、例えばユーザデバイスIDと、年齢等の各種のユーザ情報、デバイス情報を生成してサービスプロバイダ(SP12)1704に送信する((8)の処理)。この際の送信データは、先の図17を用いた説明と同様、ユーザデバイスID(UDID)と、その他サービスプロバイダ1704の求める情報(data)を含み、これらにユーザデバイス1705の秘密鍵 K_{SUD} による署名が実行され、さらに、セッション鍵 E_{Ks8} を用いて暗号化処理が実行されたデータ： $E_{Ks8}(\{UDID, data\} Sig \cdot K_{SUD})$ となる。

【0145】

サービスプロバイダ(SP12)1704は、ユーザデバイス1705から受信した暗号化データをセッション鍵 E_{Ks} で復号して、さらに署名検証を行ない、データ内容を審査して、サービスプロバイダ(SP12)1704の求める審査基準を満たすものである場合は、(9)の処理、すなわち、アクセス制御サーバ登録サーバ(RACS1)1702に対してアクセス許可書の発行依頼を行なう。

【0146】

この(9)の処理において、送信されるデータは、前述の図17の(2)の処理と同様であり、 $E_{Ks9}(\{SPID, data2\} Sig \cdot K_{SSP})$ となる。アクセス制御サーバ登録サーバ(RACS1)1702が上記データをサービスプ

ロバイダ (SP12) 1704 から受信すると、受信データに基づいてアクセス制御サーバ登録サーバ (RACS1) 1702 は、アクセス制御サーバ (ACS1) 1701 にアクセス許可書の発行要求を行なう ((10) の処理)。

【0147】

次に、アクセス制御サーバ (ACS1) 1701 は、要求データに基づいてアクセス許可書 (ACPMS) を生成し、アクセス制御サーバ (ACS1) 1701 の署名を実行したデータ: $\{ACPMS\} \text{Sig} \cdot K_{SACS1}$ をアクセス制御サーバ登録サーバ (RACS1) 1702 に送信する ((11) の処理)。なお、アクセス制御サーバ (ACS1) 1701 の生成するアクセス許可書は、先に図9, 10を用いて説明したように、複数の方式があり、例えば図9の方式Aに従う場合は、各サービスプロバイダ毎のアクセス許可書となり、この場合は、サービスプロバイダ (SP12) 1704 にのみ有効な新たなアクセス許可書を発行する。図9の方式Bに従う場合は、すでにユーザデバイス1705の有する既存のアクセス許可書に新たなサービスプロバイダ (SP12) 1704 のオプションフィールド (図10, 11参照) を付加して既存のアクセス許可書の変更処理を実行する。

【0148】

次に、アクセス制御サーバ登録サーバ (RACS1) 1702 は、アクセス制御サーバ (ACS1) 1701 からの受信データの署名検証処理を実行して、自分の署名を付加し、さらにセッション鍵で暗号化したデータ: $E_{Ks12}(\{ \{ACPMS\} \text{Sig} \cdot K_{SACS1} \} K_{SRACS1})$ をサービスプロバイダ (SP12) 1704 に送信する ((12) の処理)。

【0149】

次に、サービスプロバイダ (SP12) 1704 は、アクセス制御サーバ登録サーバ (RACS1) 1702 からの受信データの署名検証処理を実行して、自分の署名を付加し、さらにセッション鍵で暗号化したデータ: $E_{Ks13}(\{ \{ \{ACPMS\} \text{Sig} \cdot K_{SACS1} \} K_{SRACS1} \} K_{SSP})$ をユーザデバイス1705に送信する ((13) の処理)。

【0150】

ユーザデバイス 1705 は、セッション鍵 E_{Ks13} での復号処理の後、署名検証を実行し、アクセス許可書 (ACPMs) を自身のセキュアモジュールに格納する。なお、格納の際には、自身の保存鍵 K_{str} を用いて暗号化処理を行なって保存することが望ましい。この場合のアクセス許可書は、方式 A の形式の場合は、図 18 の上段に示すように各サービスプロバイダ毎のアクセス許可書となり、方式 B の場合は、図 18 の下段に示すように複数のサービスプロバイダに共通のアクセス許可書となる。

【0151】

(アクセス許可書の利用)

次に、ユーザデバイスがアクセス許可書を利用してサービスプロバイダからサービス提供を受ける処理について説明する。

【0152】

ユーザデバイスは、サービス提供を受けようとするサービスプロバイタとの間で、まず相互認証処理を実行する。相互認証処理が成立し、セッション鍵 E_{Ks} が生成されると、ユーザデバイスは、アクセス許可書 (ACPMs) に自身の秘密鍵で署名を行ない、かつセッション鍵で暗号化したデータ: $E_{Ks}(\{UDID, ACPMS\} \text{Sig} \cdot K_{SUD})$ をサービスプロバイダに送信する。

【0153】

サービスプロバイダは、受信データをセッション鍵 E_{Ks} で復号し、さらに署名検証処理を行ない、アクセス許可書 (ACPMs) のチェックを実行して、有効なアクセス許可書であることの確認を行ない、確認されたことを条件としてアクセスを許可する。

【0154】

このように、本発明のアクセス制御システムによれば、例えば複数のサービスプロバイダに共通に利用されるアクセス制御サーバが設置され、アクセス制御サーバが規定するフォーマット、手順に従ってアクセス制御が実行されることになるので、各サービスプロバイダは、独自のアクセス制御手順を構築する必要がない。また、各ユーザデバイスにおいても個々のサービスプロバイダに応じたアクセス処理シーケンスを実行することなく、一定シーケンスに従った処理が可能と

なるので、サービスプロバイダ毎のフォーマットデータ、アクセスプログラム等を個別に格納管理する必要がなくなる。

【0155】

(アクセス許可書の利用停止処理)

次に、ユーザデバイスがアクセス許可書を利用したサービスプロバイダからのサービス停止を行なう場合の処理について図19を用いて説明する。

【0156】

まず、(21)の処理は、デバイス1705がサービスプロバイダ(SP11)1703のサービス停止処理を実行するため、サービスプロバイダ(SP11)1703求めるデータを生成してサービスプロバイダに送信する。なお、送信データは、ユーザデバイスID(UDID)と、その他サービスプロバイダ1703の求める情報(data)を含み、これらにユーザデバイス1705の秘密鍵 K_{SUD} による署名が実行され、さらに、セッション鍵 E_{Ks21} を用いて暗号化処理が実行されたデータ： $E_{Ks21}(\{UDID, data\}Sig \cdot K_{SUD})$ となる。

【0157】

サービスプロバイダ(SP11)1703は、ユーザデバイス1705から受信した暗号化データをセッション鍵 E_{Ks21} で復号して、さらに署名検証を行ない、データ内容を審査して、(22)の処理、すなわち、アクセス制御サーバ登録サーバ(RACS1)1702に対してアクセス許可書の削除または変更依頼を行なう。この削除または変更処理態様は、アクセス許可書が前述の図9で説明した方式Aのサービスプロバイダ毎のアクセス許可書である場合は、許可書削除処理として実行可能であり、方式Bの場合は、アクセス許可書変更処理として実行可能である。ただし、削除の場合も例えば一定期間のアクセス停止、あるいは限定された利用のみ可能とする当、様々なアクセス不許可態様があり、許可書自体を削除することなく、許可書にアクセス制限を示す識別子を付加する処理も可能であるので、以下ではアクセス許可書の削除についても変更処理の一態様であるとして説明する。

【0158】

アクセス制御サーバ登録サーバ (RACS1) 1702 が上記データをサービスプロバイダ (SP11) 1703 から受信すると、受信データに基づいてアクセス制御サーバ登録サーバ (RACS1) 1702 は、アクセス制御サーバ (ACS1) 1701 にアクセス許可書の変更処理要求を行なう ((23) の処理)。

【0159】

次に、アクセス制御サーバ (ACS1) 1701 は、要求データに基づいてアクセス許可書 (ACPMs) の変更処理を実行し、変更したアクセス許可書にアクセス制御サーバ (ACS1) 1701 の署名を実行したデータを生成して、アクセス制御サーバ登録サーバ (RACS1) 1702 に送信する ((24) の処理)。

【0160】

次に、アクセス制御サーバ登録サーバ (RACS1) 1702 は、アクセス制御サーバ (ACS1) 1701 からの受信データの署名検証処理を実行して、自分の署名を付加し、さらにセッション鍵で暗号化した変更アクセス許可書をサービスプロバイダ (SP11) 1703 に送信する ((25) の処理)。

【0161】

次に、サービスプロバイダ (SP11) 1703 は、アクセス制御サーバ登録サーバ (RACS1) 1702 からの受信データの署名検証処理を実行して、自分の署名を付加し、さらにセッション鍵で暗号化した変更アクセス許可書をユーザデバイス 1705 に送信する ((26) の処理)。

【0162】

ユーザデバイス 1705 は、セッション鍵での復号処理の後、署名検証を実行し、変更アクセス許可書の確認を行ない、変更アクセス許可書に有効なデータがある場合は、自身のセキュアモジュールに格納する ((27) の処理)。

【0163】

(アクセス許可書の失効処理)

上述した処理は、ユーザデバイスが自らアクセス許可書の利用を停止する処理であるが、次に、サービスプロバイダ側から特定ユーザのアクセス許可書の利用

を停止、すなわち失効させる処理について図20を用いて説明する。

【0164】

まず、サービスプロバイダ1703は、不正ユーザの検出、あるいはユーザデバイスのアクセス条件が条件を満たさなくなったことが明らかになった場合等、そのユーザのアクセス許可書の失効処理の実行を決定する((31)の処理)。

【0165】

サービスプロバイダ(SP11)1703は、アクセス制御サーバ登録サーバ(RACS1)1702に対してアクセス許可書の変更依頼を行なう((32)の処理)。アクセス制御サーバ登録サーバ(RACS1)1702が上記データをサービスプロバイダ(SP11)1703から受信すると、受信データに基づいてアクセス制御サーバ登録サーバ(RACS1)1702は、アクセス制御サーバ(ACS1)1701にアクセス許可書の変更処理要求を行なう((33)の処理)。

【0166】

次に、アクセス制御サーバ(ACS1)1701は、要求データに基づいてアクセス許可書(ACPMS)の変更処理を実行し、変更したアクセス許可書にアクセス制御サーバ(ACS1)1701の署名を実行したデータを生成して、アクセス制御サーバ登録サーバ(RACS1)1702に送信する((34)の処理)。

【0167】

次に、アクセス制御サーバ登録サーバ(RACS1)1702は、アクセス制御サーバ(ACS1)1701からの受信データの署名検証処理を実行して、自分の署名を付加し、さらにセッション鍵で暗号化した変更アクセス許可書をサービスプロバイダ(SP11)1703に送信する((35)の処理)。

【0168】

このような処理の後、ユーザデバイス1705からのアクセス要求があった場合((36)の処理)は、サービスプロバイダ(SP11)1703は、変更アクセス許可書をユーザデバイス1705に送信する((37)の処理)。ユーザデバイス1705は、変更アクセス許可書の確認を行ない、有効データを含む変

更アクセス許可書がある場合は、自身のセキュアモジュールに格納する（（38）の処理）。

【0169】

（システムホルダによるアクセス許可書の失効処理）

上述した処理は、サービスプロバイダ側から特定ユーザのアクセス許可書の利用を停止、すなわち失効させる処理であったが、次にシステムホルダによるアクセス許可書の失効処理について図21を用いて説明する。

【0170】

まず、システムホルダ2101は、不正ユーザの検出、あるいはユーザデバイスのアクセス条件が条件を満たさなくなったことが明らかになった場合等、そのユーザのアクセス許可書の失効処理の実行を決定する（（41）の処理）。

【0171】

システムホルダ2101は、アクセス制御サーバ登録サーバ（RACS1）1702に対してアクセス許可書の変更依頼を行なう（（42）の処理）。アクセス制御サーバ登録サーバ（RACS1）1702が上記データをシステムホルダ2101から受信すると、受信データに基づいてアクセス制御サーバ登録サーバ（RACS1）1702は、アクセス制御サーバ（ACS1）1701にアクセス許可書の変更処理要求を行なう（（43）の処理）。

【0172】

次に、アクセス制御サーバ（ACS1）1701は、要求データに基づいてアクセス許可書（ACPMs）の変更処理を実行し、変更したアクセス許可書にアクセス制御サーバ（ACS1）1701の署名を実行したデータを生成して、アクセス制御サーバ登録サーバ（RACS1）1702に送信する（（44）の処理）。

【0173】

次に、アクセス制御サーバ登録サーバ（RACS1）1702は、アクセス制御サーバ（ACS1）1701からの受信データの署名検証処理を実行して、自分の署名を付加し、さらにセッション鍵で暗号化した変更アクセス許可書を、管轄下のサービスプロバイダ（SP11）1703、サービスプロバイダ（SP1

2) 1704に送信する((45)の処理)。

【0174】

このような処理の後、ユーザデバイス1705からのアクセス要求があった場合((46)の処理)は、サービスプロバイダ(SP11)1703は、変更アクセス許可書をユーザデバイス1705に送信する((47)の処理)。ユーザデバイス1705は、変更アクセス許可書の確認を行ない、有効データを含む変更アクセス許可書がある場合は、自身のセキュアモジュールに格納する((48)の処理)。

【0175】

[その他のエンティティ間でのアクセス許可書の利用態様]

なお、上述の例ではサービスプロバイダとユーザデバイス間でのアクセス制御について説明したが、システムホルダとサービスプロバイダ間のように異なるエンティティ間でのアクセス制御にも同様に適用可能である。また、ユーザデバイス相互間でのアクセス制御にも同様に適用できる。例えば一定のフォーマットに従ったアクセス許可書をデバイス相互間でのアクセス時に送受信する構成とすることにより、各ユーザデバイスは、一定のフォーマットに従った送信相手の情報を入手して、アクセス許可書に従ってアクセスの可否を決定することが可能となる。この場合のアクセス許可書は、図10で説明したアクセス許可書のオプションフィールドにユーザデバイスが独自に設定するフィールドを設ける構成とする。

【0176】

デバイス間でのアクセス許可書の利用態様について、図22を用いて説明する。図22において、サービスを提供するデバイス(サービス提供デバイス)をデバイス2201とし、サービスを受信するデバイス(サービス受信デバイス)をデバイス2202とする。

【0177】

まず、サービス提供デバイスであるデバイス2201は、システムホルダ2101に対して、オフラインで自分がサービス提供をしてもよいデバイス情報を含んだアクセス許可書の発行を依頼する。デバイス2201は、図10で説明した

と同様のデバイス間での流通用のアクセス許可書のオプションフィールドに、オフラインで自分がサービス提供をしてもよいデバイス情報を格納したアクセス許可書の発行を依頼する（（51）の処理）。

【0178】

また、サービス受信デバイスであるデバイス2202は、システムホルダ2101に対して、オフラインで自分がデバイス間において受けられるサービスのアクセス許可書の発行を依頼する（（52）の処理）。

【0179】

システムホルダ2101は、アクセス制御サーバ登録サーバ（RACS1）1702に対してアクセス許可書の発行依頼を行なう（（53）の処理）。アクセス制御サーバ登録サーバ（RACS1）は、アクセス制御サーバ（ACS1）1701にアクセス許可書の発行要求を行なう（（54）の処理）。

【0180】

次に、アクセス制御サーバ（ACS1）1701は、要求データに基づいてアクセス許可書を生成し、アクセス制御サーバ（ACS1）1701の署名を実行したデータをアクセス制御サーバ登録サーバ（RACS1）1702に送信する（（55）の処理）。次に、アクセス制御サーバ登録サーバ（RACS1）1702は、アクセス制御サーバ（ACS1）1701からの受信データの署名検証処理を実行して、自分の署名を付加し、さらにセッション鍵で暗号化したデータをシステムホルダ2101に送信する（（56）の処理）。

【0181】

次に、システムホルダ2101は、アクセス制御サーバ登録サーバ（RACS1）1702からの受信データの署名検証処理を実行して、自分の署名を付加し、さらにセッション鍵で暗号化したデータをデバイス2202に送信する（（57）の処理）。

【0182】

デバイス2202は、セッション鍵での復号処理の後、署名検証を実行し、アクセス許可書を自身のセキュアモジュールに格納する（（58）の処理）。

【0183】

アクセス許可書を受領したデバイス 2 2 0 2 は、デバイス 2 2 0 1 に対してアクセスする場合、アクセス許可書を提示する。デバイス 2 2 0 1 は提示されたアクセス許可書に基づいて、即座にアクセス許可、あるいは不許可を判定することが可能となる。

【 0 1 8 4 】

このデバイス間で有効なアクセス許可書についてもサービス停止処理、失効処理は、前述のサービスプロバイダのアクセス許可書の処理と同様に行なわれる。ただし、更新されたアクセス許可書の配布処理は、システムホルダからデバイスに対する配布処理となる。デバイスがシステムホルダに対して接続するタイミングは、例えば公開鍵証明書の更新処理時等であり、この際に更新されたアクセス許可書を配布することが可能である。

【 0 1 8 5 】

ただし、サービス提供デバイスがアクセス許可書が更新されたことをサービス受信デバイスに通知して、その通知以降のデバイス間のサービスのやりとりは、サービス受信デバイスがシステムホルダに対して接続がなされたことを条件とする構成とすることで、無効なアクセス許可書の使用を排除することが可能となる。

【 0 1 8 6 】

以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

【 0 1 8 7 】

【発明の効果】

上述したように、本発明のアクセス制御システムによれば、複数のサービスプロバイダ、デバイスに共通に利用されるアクセス制御サーバが設置され、アクセス制御サーバが規定するフォーマット、手順に従ってアクセス制御が実行されることになるので、各サービスプロバイダ、デバイスは、独自のアクセス制御手順

を構築する必要がなく、容易にアクセス制御を実行することが可能となる。また、サービスを受けるユーザデバイスにおいても個々のサービスプロバイダに応じたアクセス処理シーケンスを実行することなく、一定シーケンスに従った処理が可能となるので、サービスプロバイダ毎のフォーマットデータ、アクセスプログラム等を個別に格納管理する必要がなくなる。

【図面の簡単な説明】

【図 1】

公開鍵証明書 の例を示す図である。

【図 2】

本発明の公開鍵暗号を使用したデータ通信システムの概要を説明する図である。

【図 3】

公開鍵暗号を使用したデータ通信システムにおけるシステムホルダと他機関との関係について説明する図である。

【図 4】

公開鍵暗号を使用したデータ通信システムにおけるシステムホルダと他機関の具体例を説明する図である。

【図 5】

システムホルダをルート登録局に対する階層構造としない場合の公開鍵証明書利用例を説明する図である。

【図 6】

システムホルダをルート登録局に対する階層構造とした場合の公開鍵証明書利用例を説明する図である。

【図 7】

アクセス制御サーバを構成要素としたシステムの概要（例 1）を説明する図である。

【図 8】

アクセス制御サーバを構成要素としたシステムの概要（例 2）を説明する図である。

【図 9】

アクセス許可書の方式例を説明する図である。

【図 1 0】

アクセス許可書のフォーマットについて説明する図である。

【図 1 1】

アクセス許可書に含まれる内容について説明する図である。

【図 1 2】

本発明のシステムにおいて適用可能な署名生成処理について説明する図である。

【図 1 3】

本発明のシステムにおいて適用可能な署名検証処理について説明する図である。

【図 1 4】

本発明のシステムにおいて適用可能な相互認証処理について説明する図である。

【図 1 5】

本発明のシステムにおいて適用可能な相互認証処理について説明する図である。

【図 1 6】

本発明のシステムの処理において使用される用語を説明する図である。

【図 1 7】

本発明のアクセス制御システムにおける最初のアクセス許可書発行処理シーケンスを説明する図である。

【図 1 8】

本発明のアクセス制御システムにおけるアクセス許可書発行処理シーケンスを説明する図である。

【図 1 9】

本発明のアクセス制御システムにおけるアクセス許可書のサービス停止処理シーケンスを説明する図である。

【図 20】

本発明のアクセス制御システムにおけるアクセス許可書のサービス失効処理シーケンスを説明する図である。

【図 21】

本発明のアクセス制御システムにおけるアクセス許可書のシステムホルダが主体となるサービス失効処理シーケンスを説明する図である。

【図 22】

本発明のアクセス制御システムにおけるデバイス間のアクセス許可書の利用シーケンスを説明する図である。

【符号の説明】

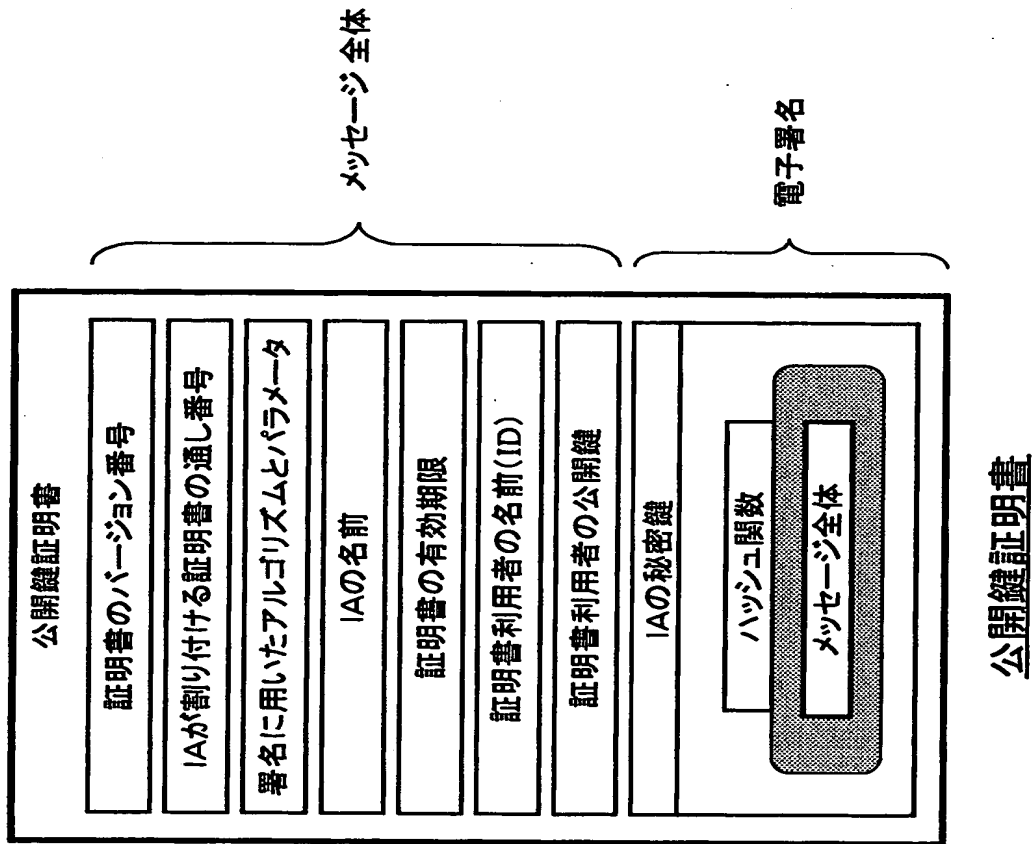
- 201 公開鍵証明書発行局 (IA)
- 202 ルート登録局 (ルートRA)
- 203, 204 登録局 (サービスプロバイダRA)
- 205 登録局 (ペイメントRA)
- 206 ショップ
- 207 端末
- 208 ユーザデバイス
- 209 ユーザの決済機関
- 301 システムホルダ (SH)
- 302 コンテンツクリエイター (CC)
- 303 サービスプロバイダ (SP)
- 304 ユーザ (デバイス)
- 511, 521 公開鍵証明書発行局 (IA)
- 512, 522 ルート登録局 (ルートRA)
- 513, 523 審査機関
- 514, 524 サービスプロバイダ
- 515, 525 ユーザ (デバイス)
- 601 公開鍵証明書発行局 (IA)
- 602 ルート登録局 (ルートRA)

603, 606 システムホルダ
604, 607 サービスプロバイダ
605, 608 ユーザ (デバイス)
701 公開鍵証明書発行局 (IA)
702 ルートRA
703, 750 システムホルダ
705, 706, 707 サービスプロバイダ
708, 709 ユーザデバイス
710 アクセス制御サーバ
720 アクセス制御サーバ登録サーバ
752 ユーザデバイス
810 アクセス制御サーバ
820 アクセス制御サーバ登録サーバ
1701 アクセス制御サーバ
1702 アクセス制御サーバ登録サーバ
1703, 1704 サービスプロバイダ
1705 ユーザデバイス
2101 システムホルダ
2201, 2202 デバイス

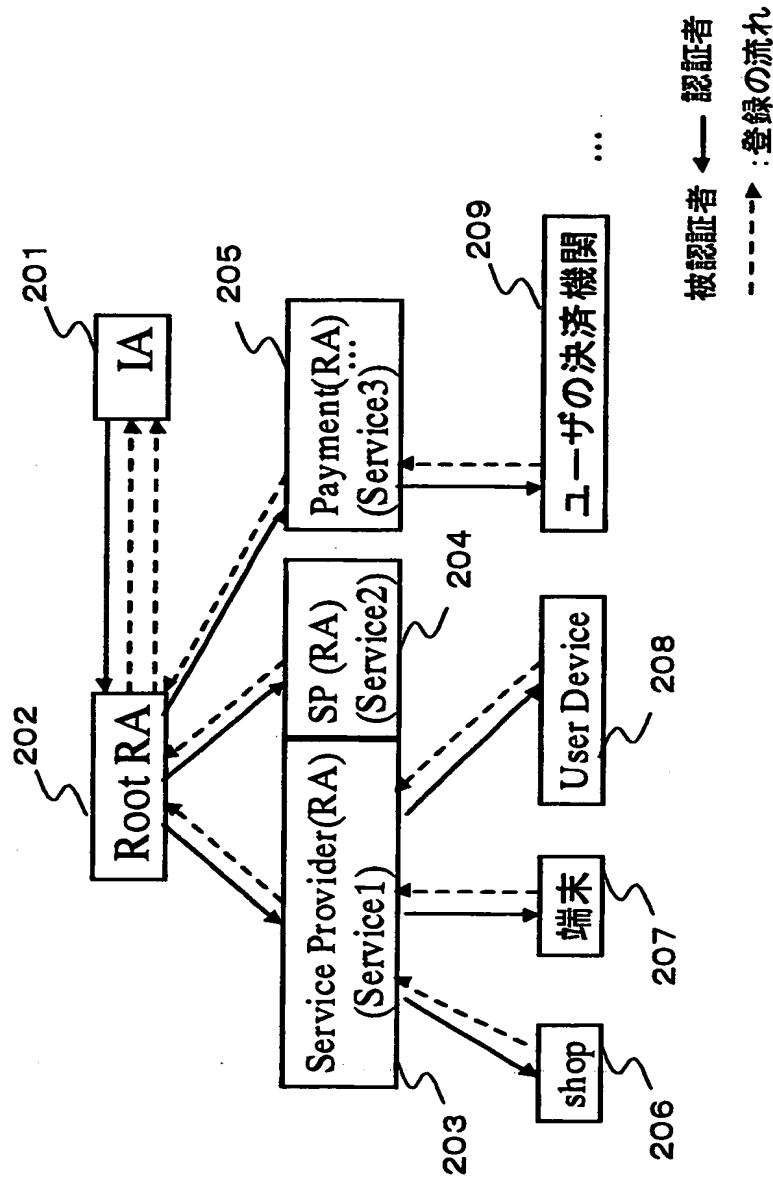
【書類名】

図面

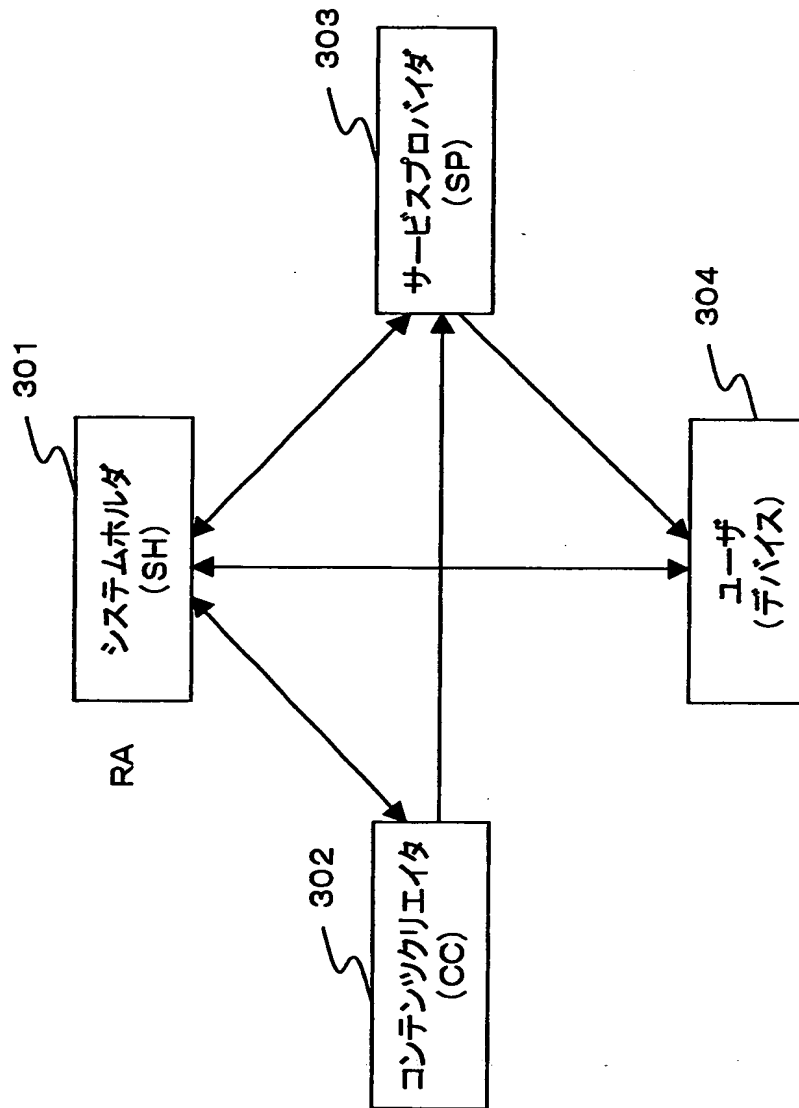
【図1】



【図 2】



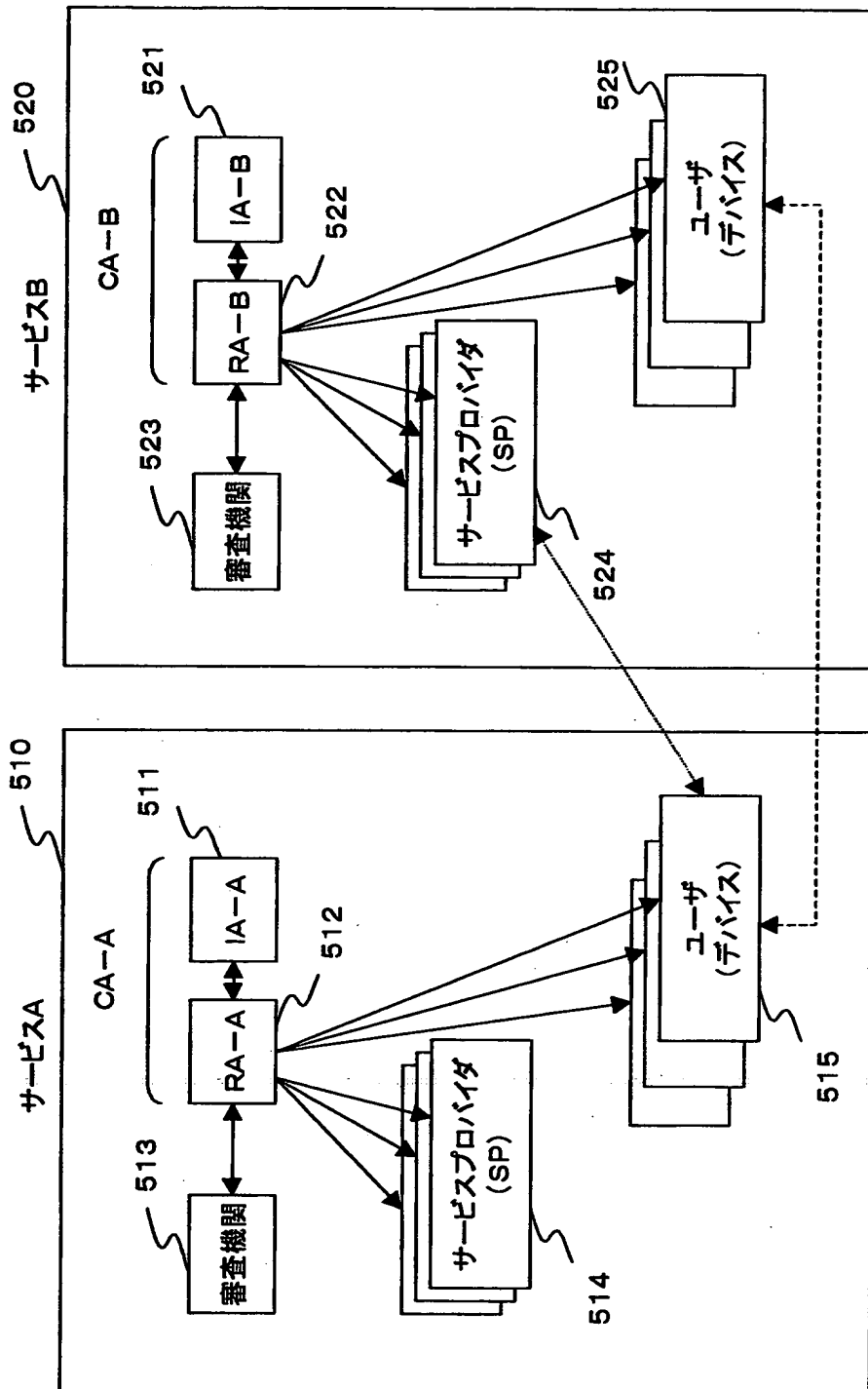
【図3】



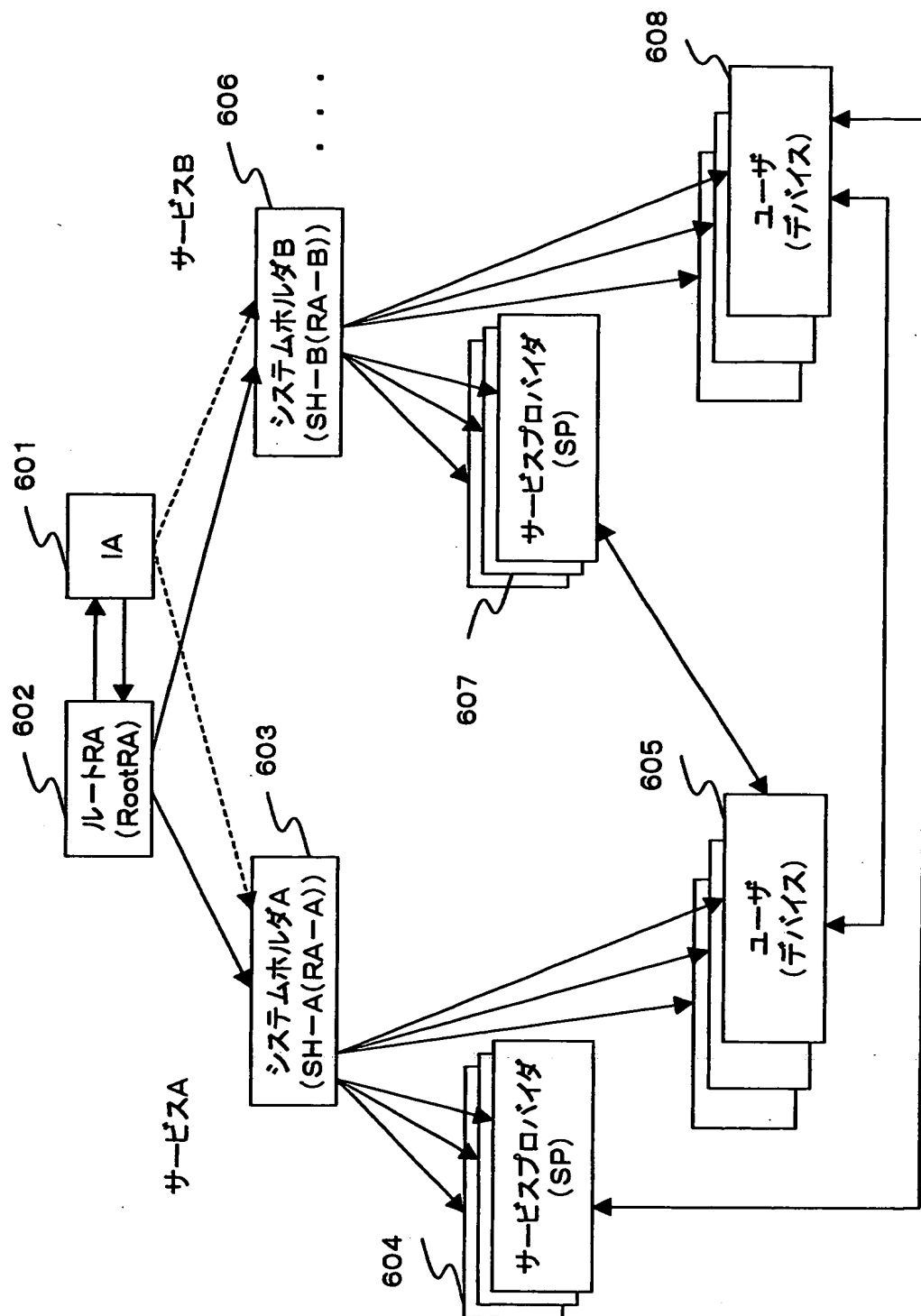
【図4】

No.	システムホルダ(SH)	コンテンツ・クリエイタ(CC)	サービスプロバイダ(SP)	ユーザデバイス
1.	インターネットショップ マーケット主催機関	マーケット提供商品、 コンテンツの生成、製造者	マーケット提供商品ショップ	PC
2.	携帯電話通信インフラ 提供機関	携帯電話インフラを利用した 提供コンテンツ、商品の生成者	携帯電話利用ユーザに対する コンテンツ配信者	携帯電話
3.	ケーブルテレビ ケーブル管理機関	ケーブルTV番組制作者	ケーブルTV会社	TV(受像機)
4.	電子マネー・カード 発行機関	電子マネーにより購入可能な 商品、コンテンツの生成者	電子マネー利用可能ショップ	ICカード
5.	:	:	:	:
6.	:	:	:	:

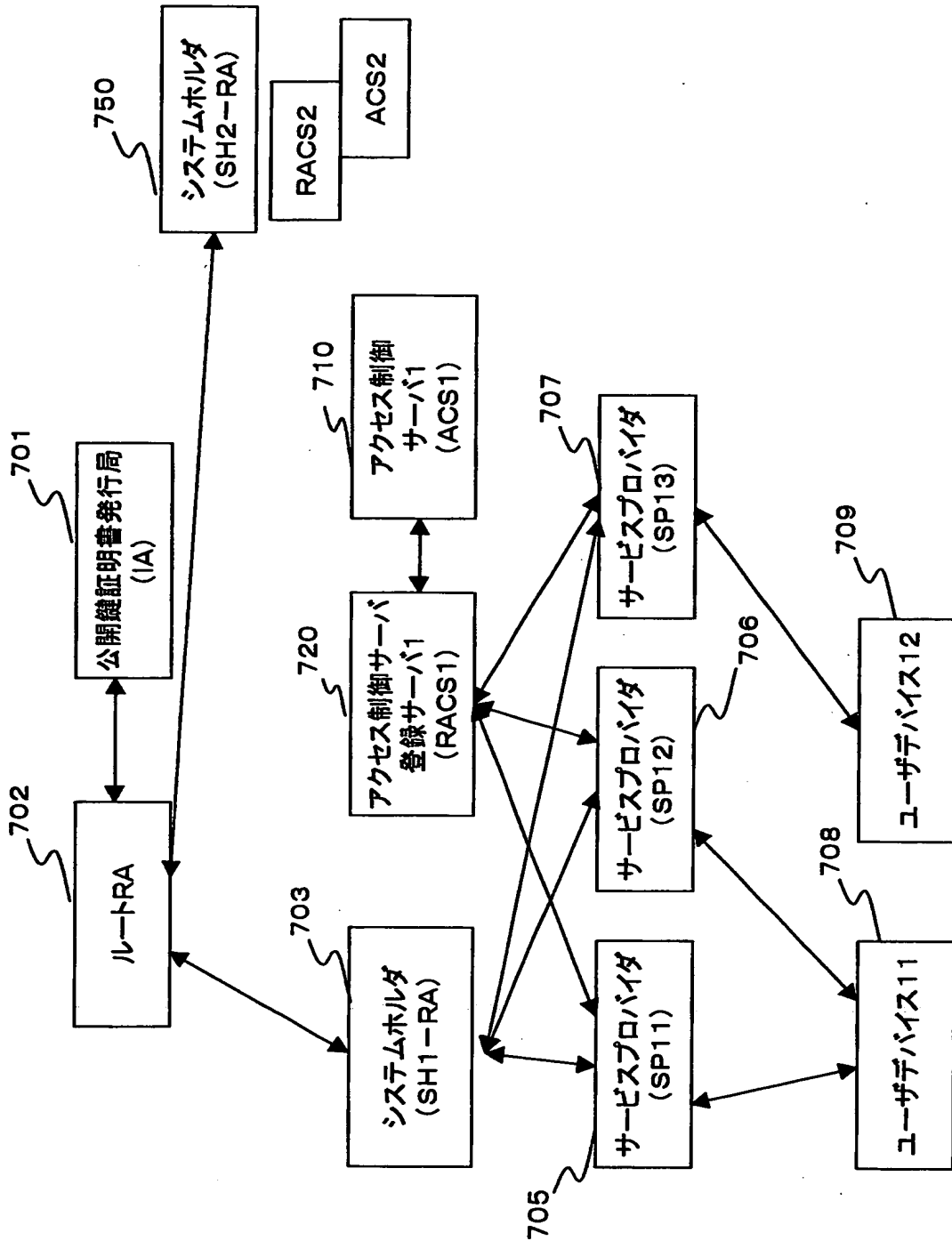
【図5】



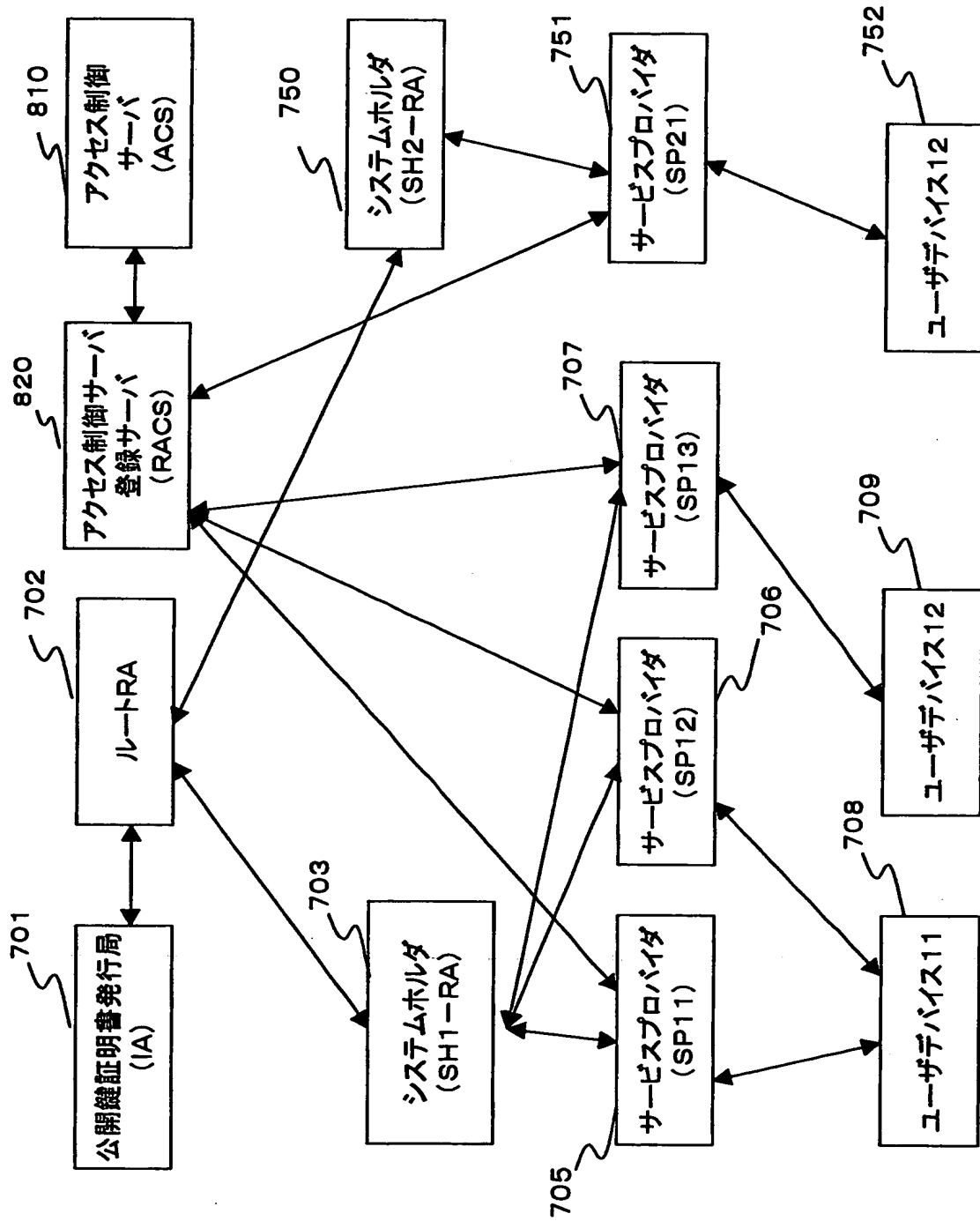
【図6】



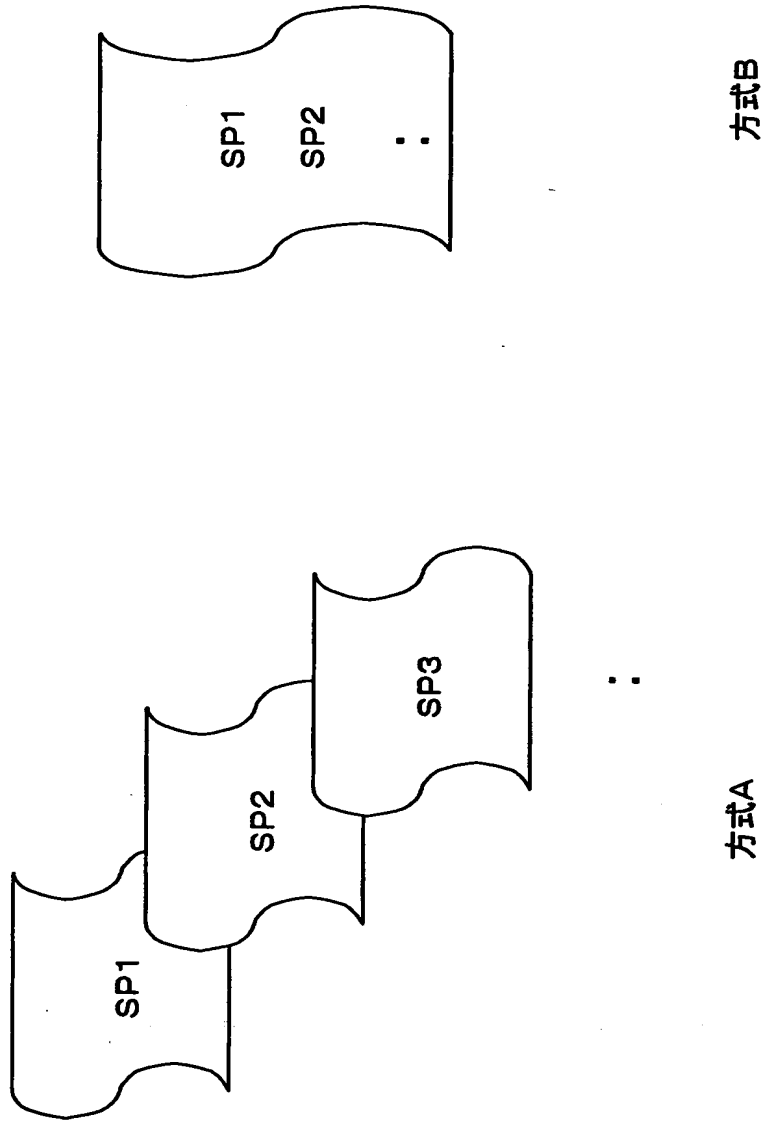
【図 7】



【図 8】



【図9】

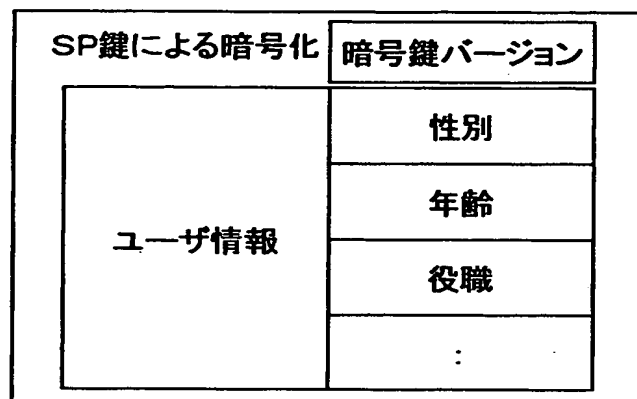


【図10】

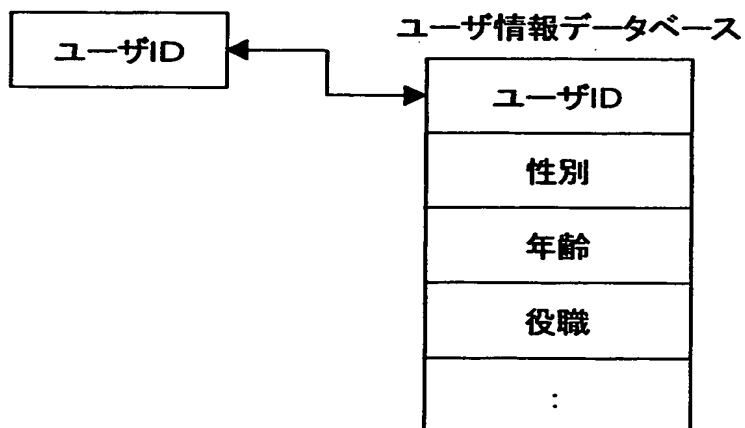
固定フィールド アクセス制御サーバ (ACS) が設定	シリアル番号		
	有効期間		
	公開鍵証明書(PKC)のシリアル番号		
	バージョン番号		
	発行者識別名		
	署名方式		
オプションフィールド 各サービスプロバイダ (SP) が設定	オプションフィールドサイズ		
	SP1	サービスプロバイダ(SP)識別名	
		データサイズ	
		内容(図11参照)	
	SP2	サービスプロバイダ(SP)識別名	
		データサイズ	
		内容(図11参照)	
	:		
	署名		
	署名フィールド(ACS)		

【図 11】

方式イ)



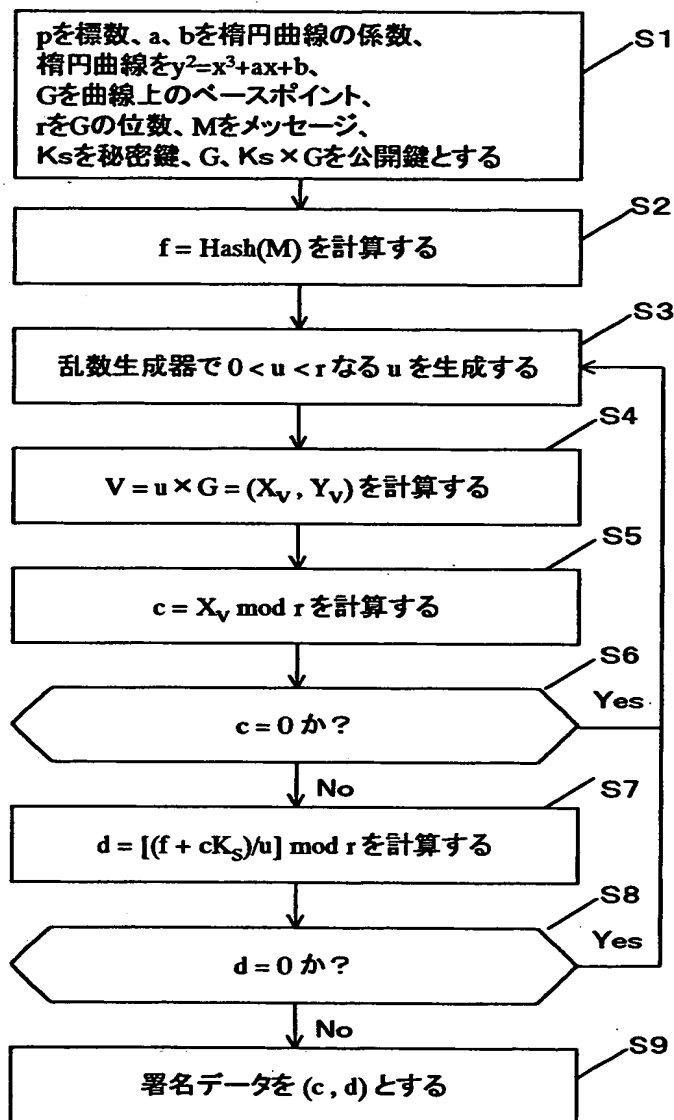
方式ロ)



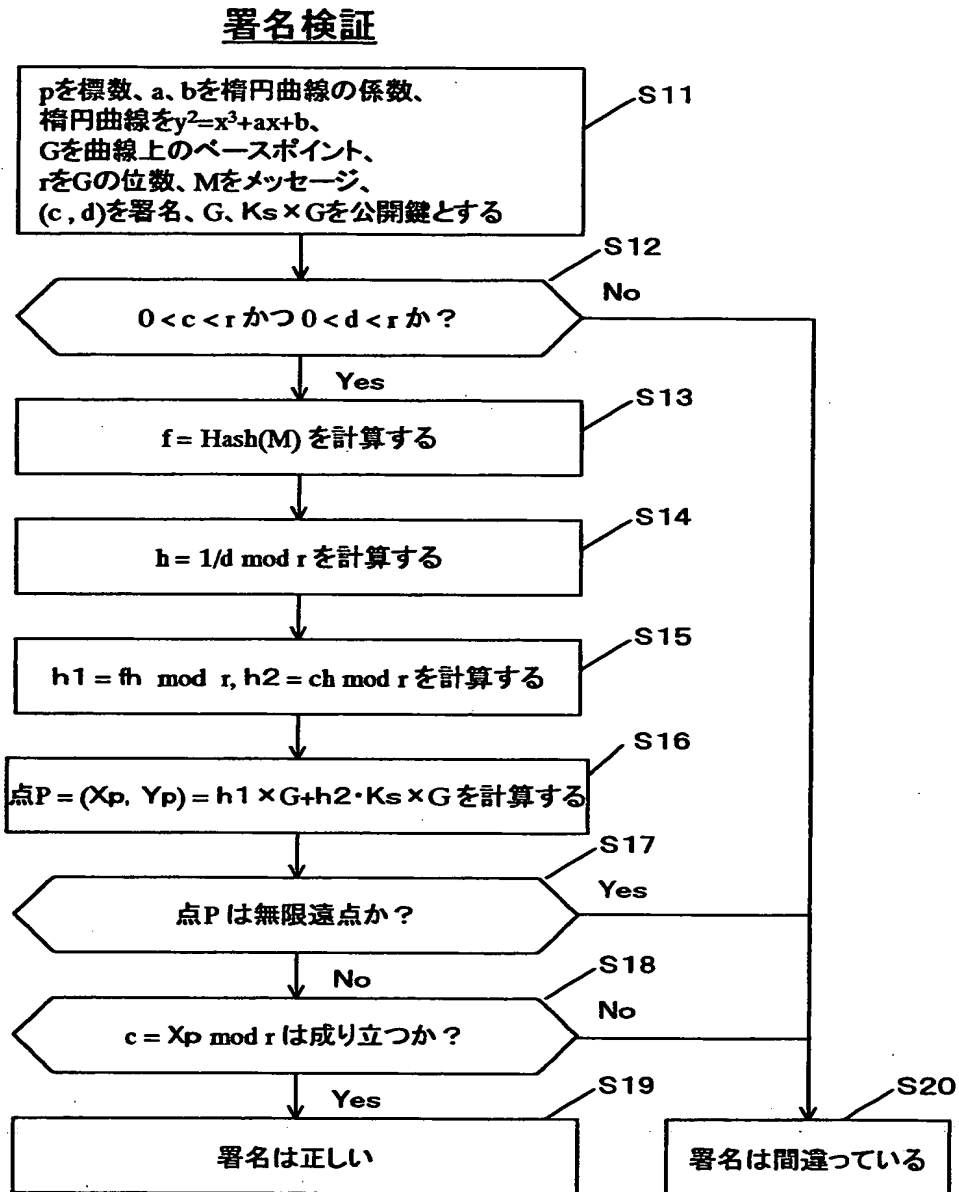
方式ハ)



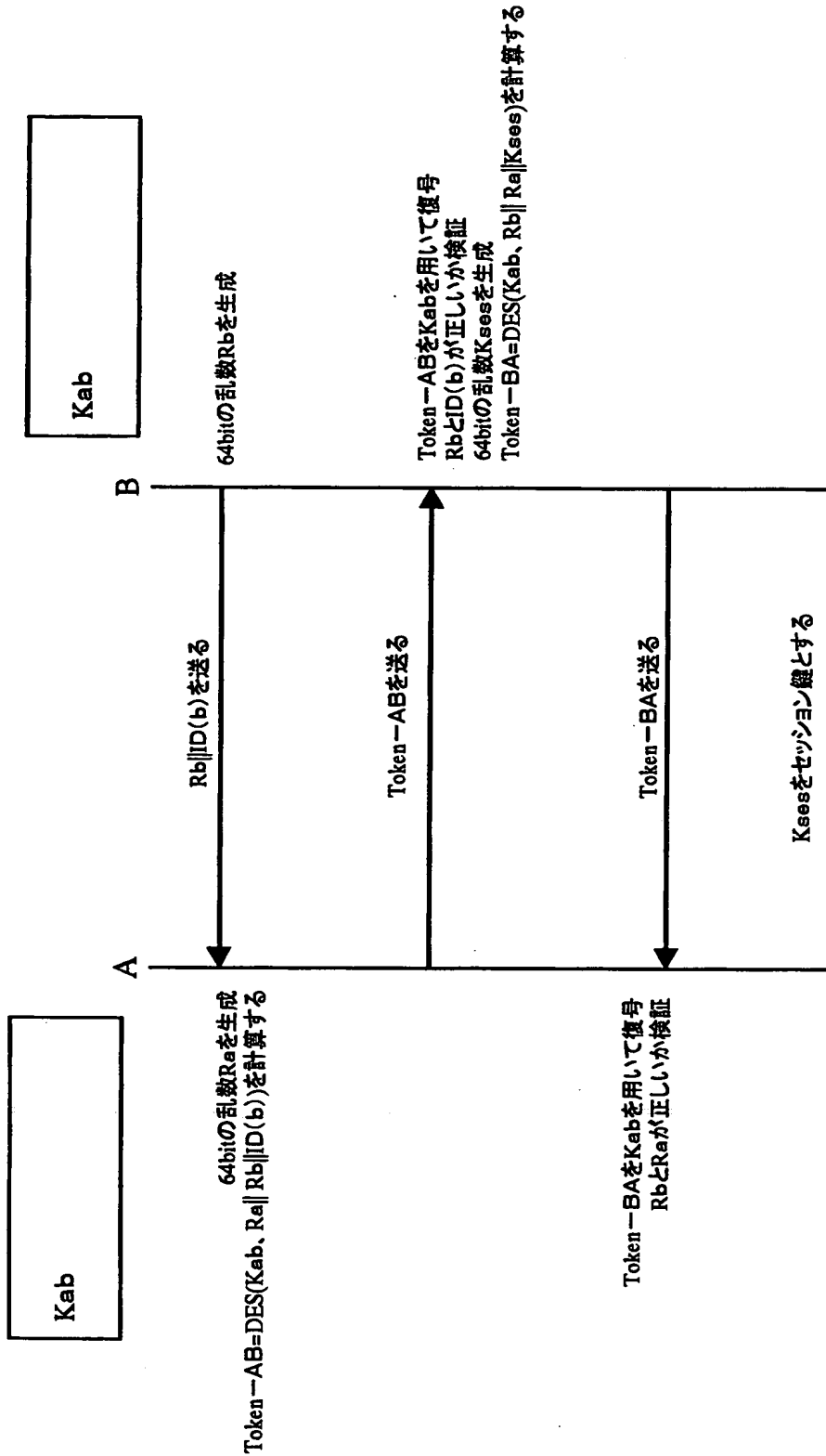
【図 12】

署名生成署名生成(IEEE P1363/D3)

【図 13】

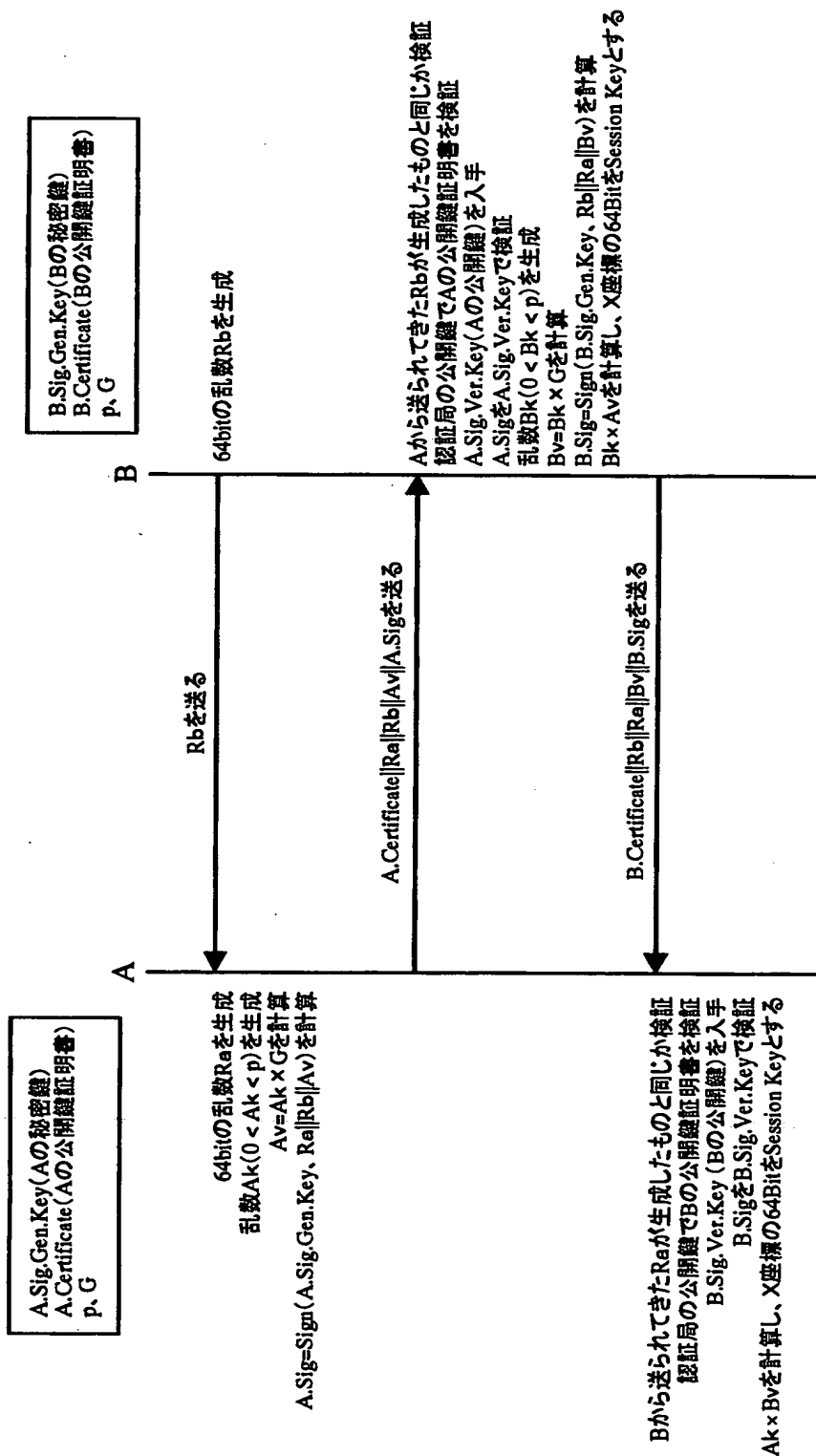
**署名検証(IEEE P1363/D3)**

【図 14】



ISO/IEC 9798-2 対称鍵暗号技術を用いた相互認証および鍵共有方式

【図 15】

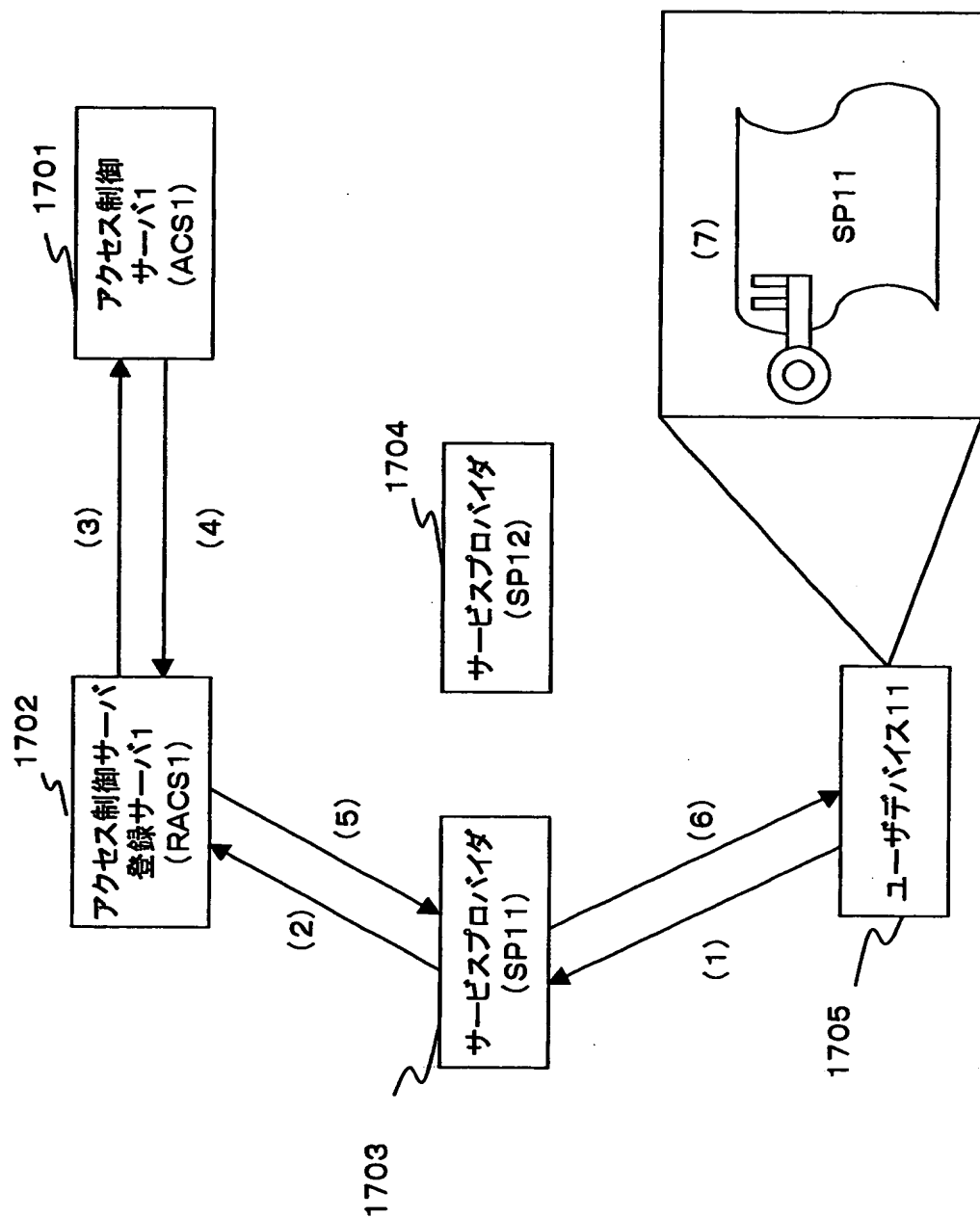


ISO/IEC 9798-3 非対称鍵暗号技術を用いた相互認証および鍵共有方式

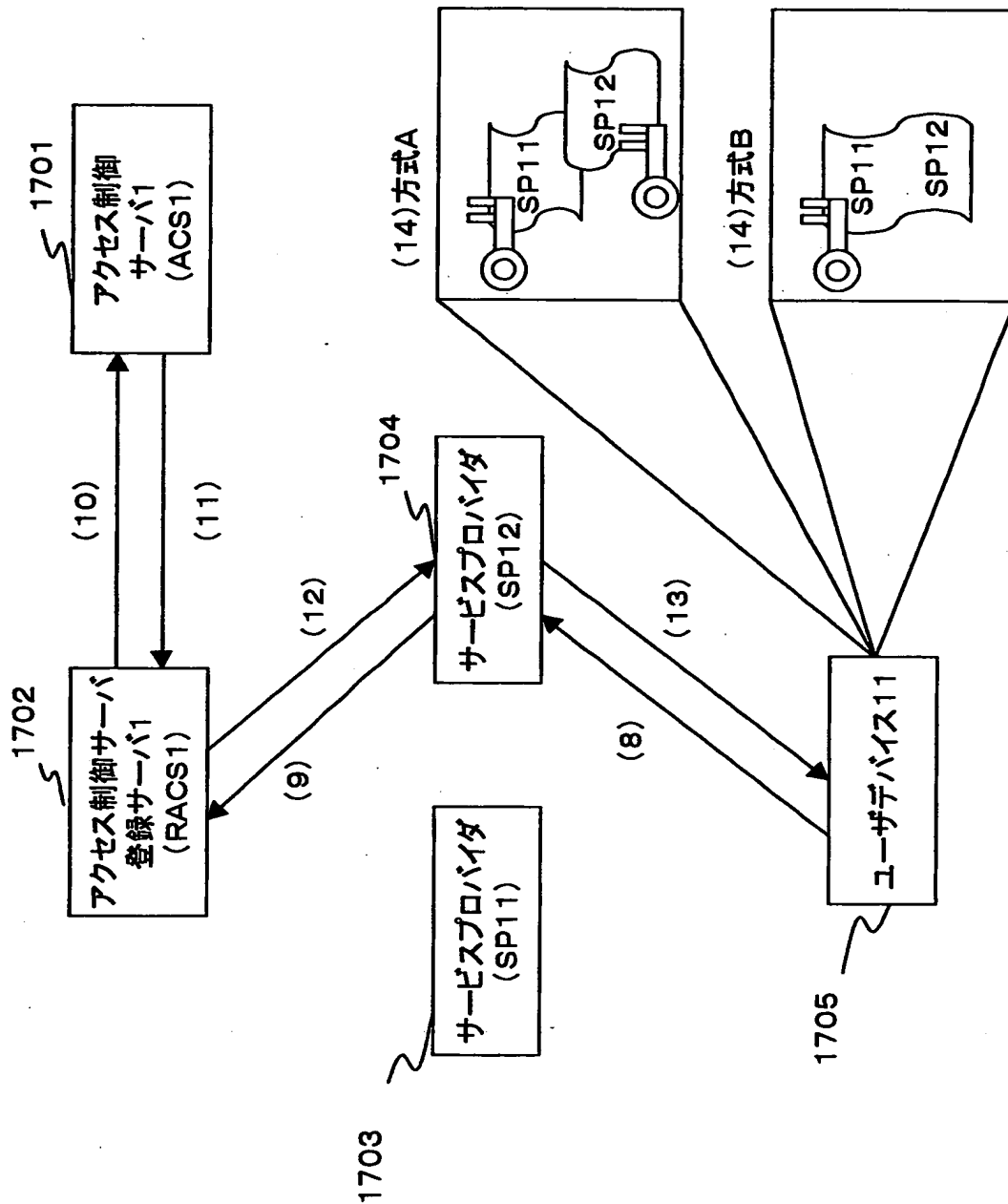
【図16】

No.	用語	記号	説明・備考
1	公開鍵	K_{Pa}	Aの公開鍵。 例 User $\rightarrow K_{Pu}$ UD $\rightarrow K_{Pud}$ SP $\rightarrow K_{Psp}$
2	秘密鍵	K_{Sa}	Aの秘密鍵。 例 User $\rightarrow K_{Su}$ UD $\rightarrow K_{Sud}$ SP $\rightarrow K_{Ssp}$
3	セッション鍵	Ks	相互認証の際、作成される共通鍵
4	証明書	$A\langle\langle B \rangle\rangle$	Aが発行したBの証明書。 例: IAによるUDの証明書 $\rightarrow IA\langle\langle UD \rangle\rangle$
5	暗号化	$E_{Ks}(data)$	平文Dataを鍵Ksで暗号化
6	復号	$D_{Ks}(data)$	暗号文dataを鍵Ksで復号
7	署名	$\{ data \} Sig. K_{Sa}$	DataをAの秘密鍵 K_{Sa} で署名
8	署名付き暗号化	$E_{Ks}(\{ data \} Sig. K_{Sa})$	dataをAの秘密 K_{Sa} で署名し、(data 署名)を鍵Ksで暗号化

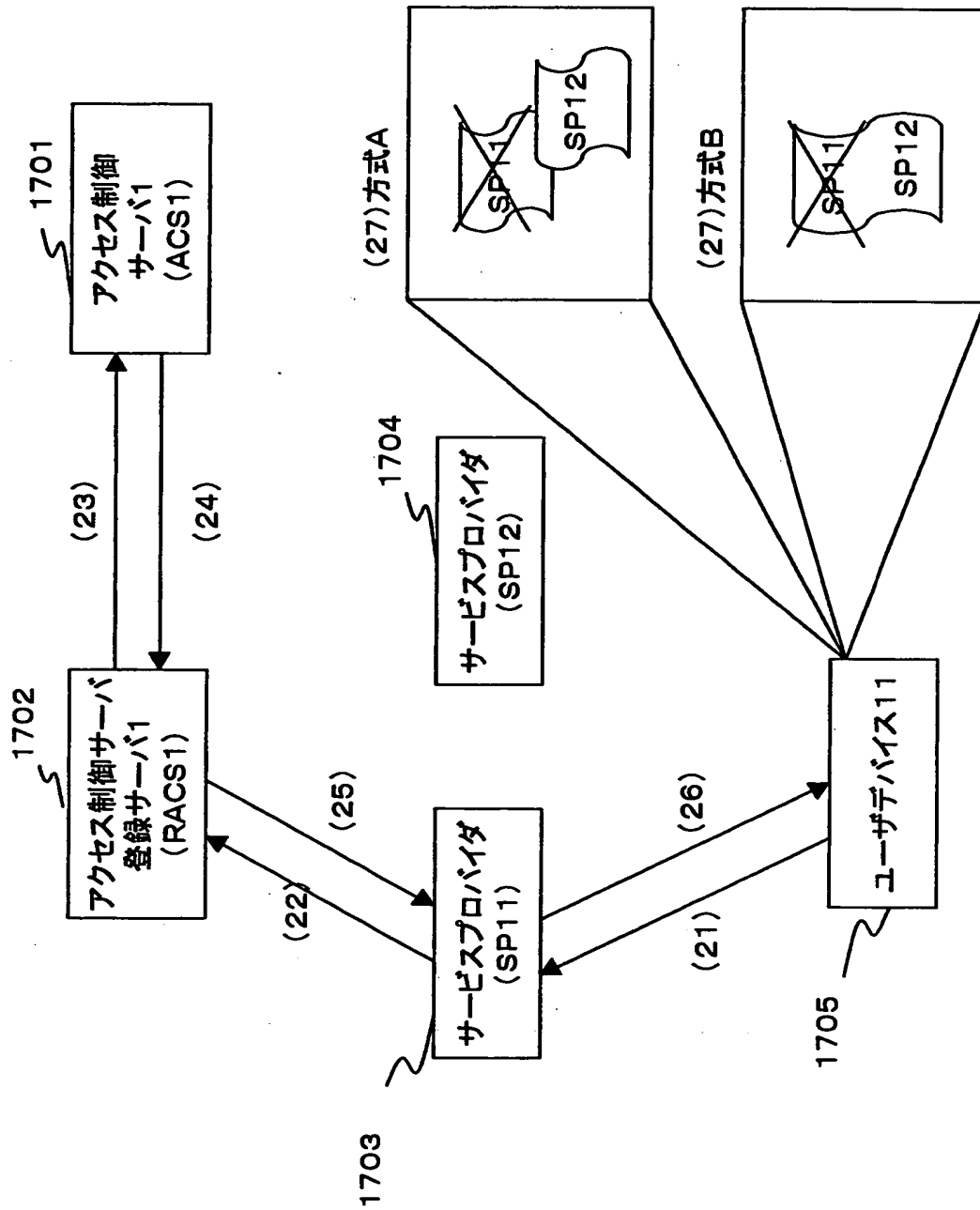
【図17】



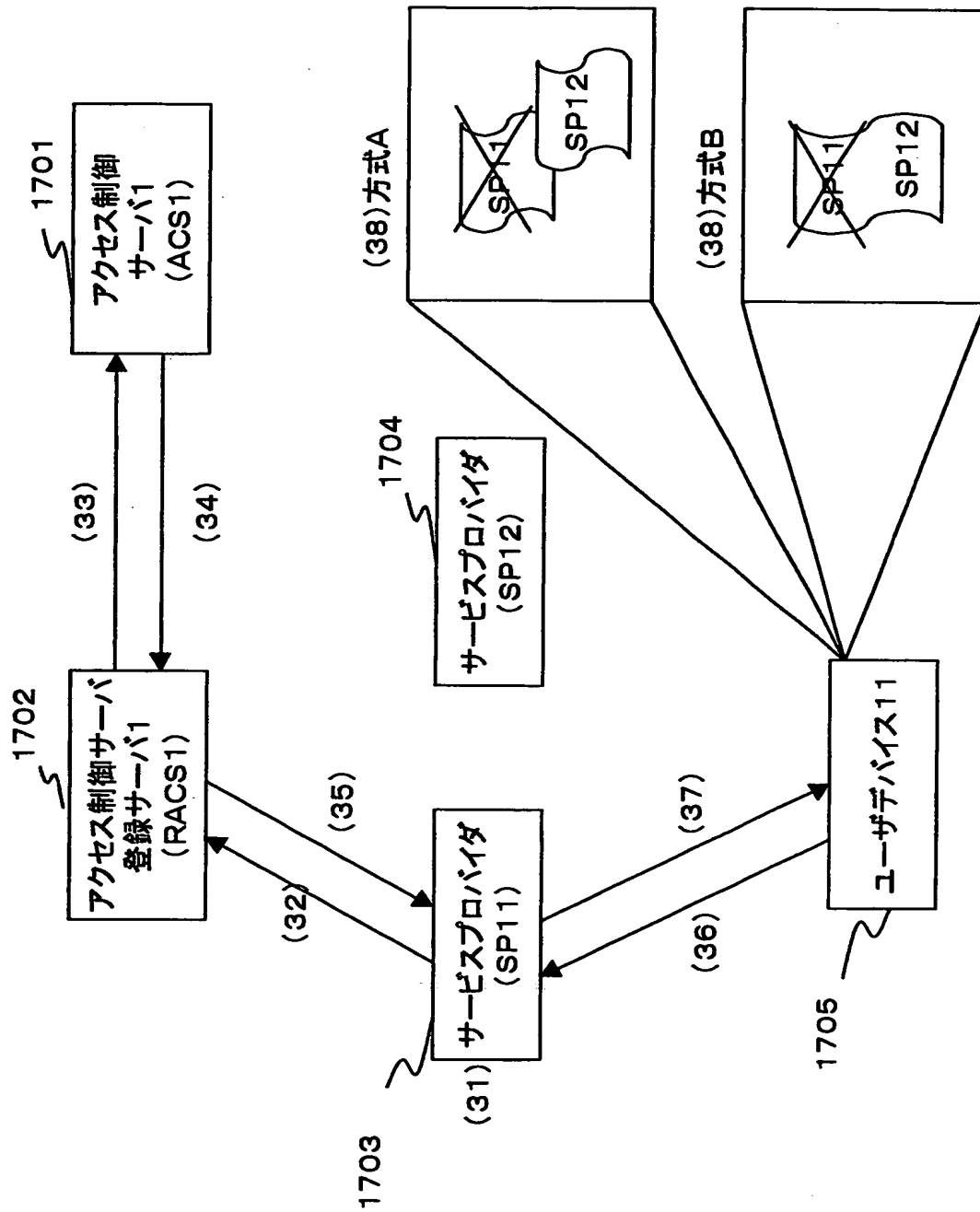
【図18】



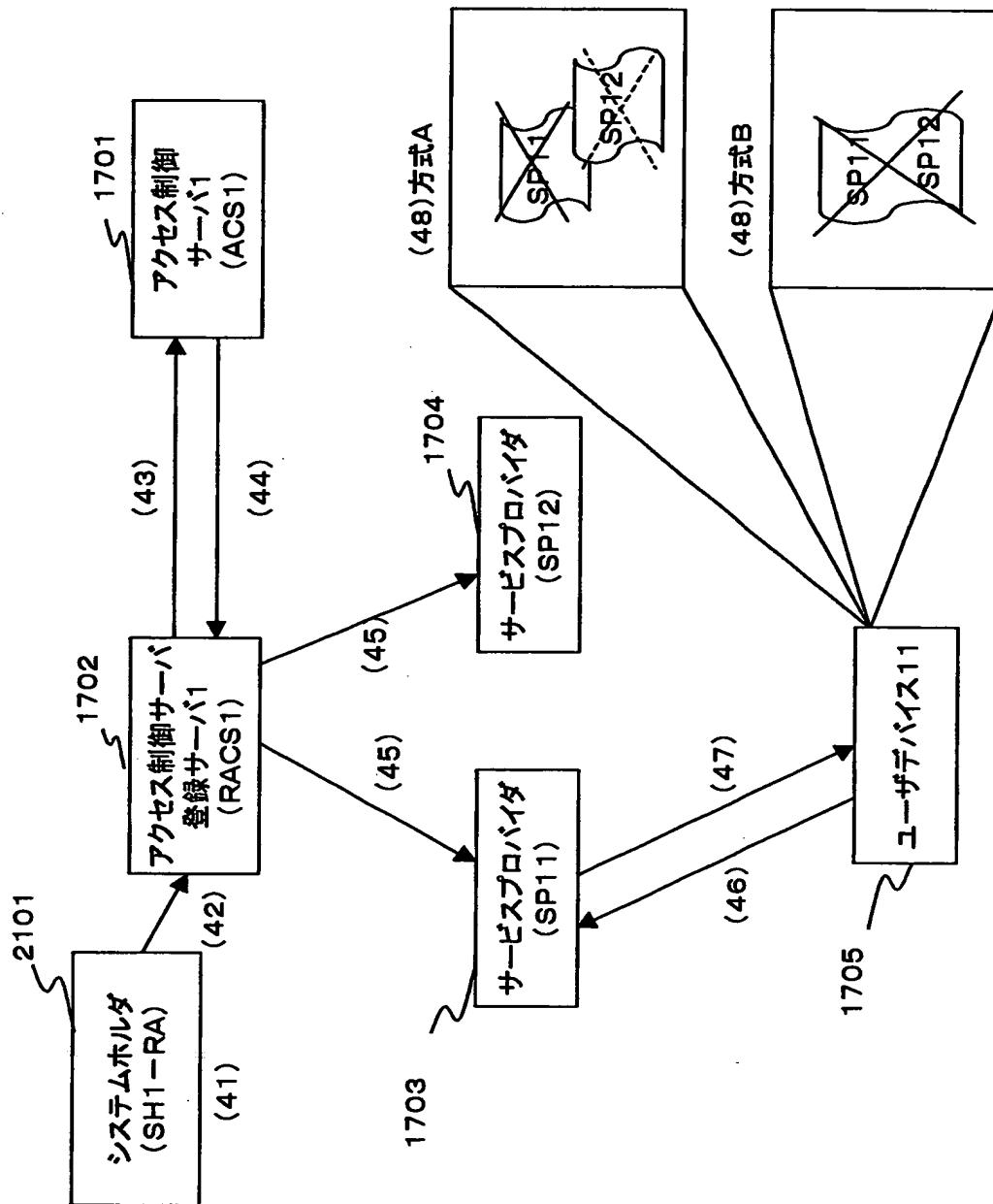
【図19】



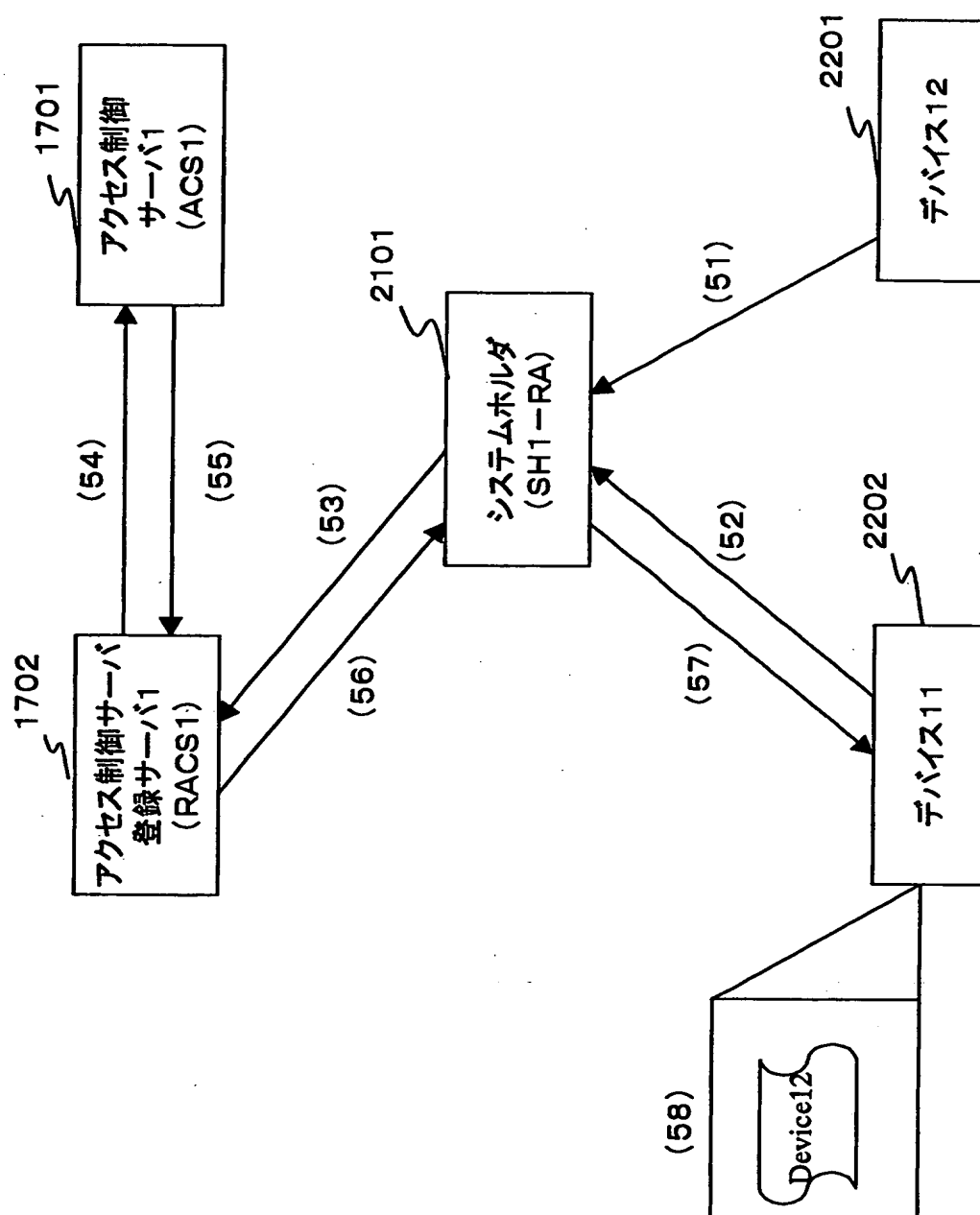
【図20】



【図 2 1】



【図 22】



【書類名】 要約書

【要約】

【課題】 サービスプロバイダが個々にアクセス制御を行なうことを不要としたアクセス制御システムを提供する。

【解決手段】 複数のサービスプロバイダ、デバイスに共通に利用されるアクセス制御サーバが設置され、アクセス制御サーバが規定するフォーマット、手順に従ったアクセス許可書を発行する。アクセス許可書に従ってアクセス制御が実行され、各サービスプロバイダ、デバイスは、独自のアクセス制御手順を構築することなく、容易にアクセス制御を実行することが可能となる。サービスを受けるユーザデバイスにおいても個々のサービスプロバイダに応じたアクセス処理シーケンスを実行することなく、一定シーケンスに従った処理が可能となるので、サービスプロバイダ毎のフォーマットデータ、アクセスプログラム等を個別に格納管理する必要がない。

【選択図】 図7

出 願 人 履 歴 情 報

識別番号 [000002185]

1. 変更年月日 1990年 8月30日

[変更理由] 新規登録

住 所 東京都品川区北品川6丁目7番35号

氏 名 ソニー株式会社